

TD ALGEBRE

LICENCE

NICE 78-79



## M1 UV algèbre et arithmétique.

## Feuille N° 1

<u>Horaires des T.D.</u>	Groupe 1	Mardi 15h45 - 17h15	Salle 1.1
		Mercredi 9h15 - 10h15	" "
	Groupe 2	Mardi 14h - 15h30	Salle 1.1
		Mercredi 10h30 - 12h	" "

## Exercices

- x 1° Soit  $G$  un groupe. Donner une condition nécessaire et suffisante pour que la réunion de sous-groupes  $H$  et  $K$  de  $G$  soit un sous-groupe de  $G$ .
- x 2° L'intersection, la réunion et la différence symétrique sont-elles des lois de groupe sur l'ensemble  $\mathcal{P}(E)$  des parties d'un ensemble  $E$  (même vide!)?
- x 3° Soit  $G$  un groupe. On considère la loi de composition interne définie sur  $\mathcal{B}(G)$  = ensemble des parties de  $G$  par
- $$(\mathcal{A}, \mathcal{B}) \mapsto \mathcal{A}\mathcal{B} = \{ab \mid a \in \mathcal{A} \text{ et } b \in \mathcal{B}\}$$
- a) Vérifiez qu'elle n'induit pas une loi de composition interne sur l'ensemble des sous-groupes de  $G$ .
- b) Si  $H$  et  $K$  sont des sous-groupes de  $G$ , prouvez que  $HK$  est un sous-groupe de  $G$  si et seulement si  $HK = KH$ .
- c) Trouvez un groupe  $G$  et deux sous-groupes  $H$  et  $K$  de  $G$  tels que  $HK$  ne soit pas un sous-groupe de  $G$ .
- d) Si  $G$  est un groupe commutatif,  $(\mathcal{A}, \mathcal{B}) \mapsto \mathcal{A}\mathcal{B}$  est-elle une loi de groupe sur l'ensemble des sous-groupes de  $G$ ?

4° a) Soit  $H$  le sous-ensemble de  $GL(\mathbb{C}^2)$  formé des matrices de la forme  $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$  avec  $\lambda \in \mathbb{C}^*$  dites homothéties de  $\mathbb{C}^2$ . Vérifiez que  $H$  est un sous-groupe distingué de  $GL(\mathbb{C}^2)$ .

Le groupe  $PGL(\mathbb{C}^2) = GL(\mathbb{C}^2)/H$  est appelé le groupe linéaire projectif de  $\mathbb{C}^2$ .

b) Soit  $SL(\mathbb{C}^2)$  le sous-ensemble de  $GL(\mathbb{C}^2)$  défini par  

$$m \in SL(\mathbb{C}^2) \Leftrightarrow \det m = 1$$

Prouvez que  $SL(\mathbb{C}^2)$  est un sous-groupe distingué dans  $GL(\mathbb{C}^2)$ , dit groupe spécial linéaire de  $\mathbb{C}^2$ .

c) On définit les sous-ensembles  $GL^+(\mathbb{R}^2)$  et  $GL^-(\mathbb{R}^2)$  de  $GL(\mathbb{R}^2)$  par  

$$m \in GL^+(\mathbb{R}^2) \Leftrightarrow \det m > 0$$

$$m \in GL^-(\mathbb{R}^2) \Leftrightarrow \det m < 0.$$

Sont-ce des sous-groupes distingués de  $GL(\mathbb{R}^2)$ ?

x 5° Soit  $E$  un espace vectoriel sur un corps commutatif  $k$ .

Montrer que le centre de  $GL(E)$  (i.e l'ensemble des automorphismes qui commutent avec tous les autres) est l'ensemble des homothéties de  $E$  de rapport non nul.

x 6° Soient  $n$  et  $m$  deux entiers supérieurs à 1. Étudiez  
 $\text{Hom}(\mathbb{Z}, \mathbb{Z})$ ,  $\text{Hom}(\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ ,  $\text{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})$  et  
 $\text{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ ; (on remarquera qu'un homomorphisme est défini, ici, par la valeur qu'il prend en 1).

7° Soit  $G$  le groupe (à vérifier, après avoir défini une loi...) des transformations bijectives affines de  $\mathbb{R}$   
 (i.e des applications  $f: \mathbb{R} \rightarrow \mathbb{R}$  définies par  $f(x) = ax + b$ ,  $a \neq 0$ ).

Montrer que l'ensemble  $H$  des homothéties (multiplication par un scalaire) est un sous-groupe <sup>non distingué</sup> distingué de  $G$ , et que le groupe  $G/H$  est isomorphe au groupe des translations.

Montrer que le groupe des translations  $T$  est un sous-groupe distingué de  $G$ .

①

Montrons que

$$\{ H \cup K = \text{o. groupe de } G \} \Leftrightarrow \{ H \subset K \text{ ou } K \subset H \}$$

 $(\Leftarrow)$  évident.

$$(\Rightarrow) \text{ Supposons, par l'absurde, que } \begin{cases} H \not\subset K \\ \text{et} \\ K \not\subset H \end{cases} \Leftrightarrow \begin{cases} \exists x \in H \setminus K \\ \exists y \in K \setminus H \end{cases}$$

Comme la loi  $\cdot$  est interne dans  $H$ ,  $x, y \in H \cup K$ . Supposons, par exemple (ce qui ne restreint pas la généralité) que  $xy \in H$ .

$$\bullet \text{ Plus } xy = h \in H \Rightarrow y = \underbrace{x^{-1}}_{\in H} \underbrace{h}_{\in H} \Rightarrow y \in H$$

Or  $y \in K \setminus H$ , d'où l'absurdité.

② Considérons  $\mathcal{P}(E)$ 

a)  $(\mathcal{P}(E), \cap)$  ~~est~~ groupe ~~abélien~~ (pas d'élément symétrique) sauf si  $E = \emptyset$   
 $(\mathcal{P}(\emptyset), \cap) = \text{groupe commutatif}$

b)  $(\mathcal{P}(E), \cup)$   $\neq$  groupe

$$= \{\emptyset\}$$

$\emptyset$  = le "prétendant" élément neutre

$\bullet$  Soit  $A \neq \emptyset$   $A \in \mathcal{P}(E)$ . Soit  $A'$  tel que  $A \cup A' = \emptyset$  (si  $A'$  existe)  
 mais  $A \cup A' \supset A \Rightarrow A \cup A' \neq \emptyset \quad \forall A'$

$\nexists A^{-1}$

c)  $(\mathcal{P}(E), \Delta)$

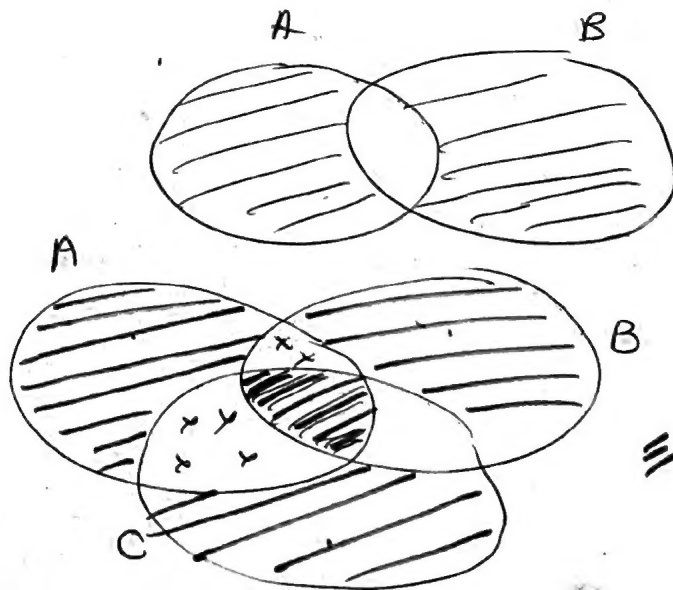
$$= (A \cup B) \setminus (A \cap B)$$

$$A \Delta B = (A \setminus B) \cup (B \setminus A)$$

$$= (A \cup B) \setminus (A \cap B)$$

$\Delta$  est interne

$\Delta$  associatif



$$\equiv (A \Delta B) \Delta C$$



1-méthode

$$A \Delta B = (A \cap \bar{B}) \cup (\bar{A} \cap B)$$

$$\begin{aligned} (A \Delta B) \Delta C &= \{ [(A \cap \bar{B}) \cup (\bar{A} \cap B)] \cap \bar{C} \} \cup \{ \overline{[(A \cap \bar{B}) \cup (\bar{A} \cap B)] \cap C} \} \\ &= \{ (A \cap \bar{B} \cap \bar{C}) \cup (\bar{A} \cap B \cap \bar{C}) \} \cup \{ \underbrace{[(\bar{A} \cup B) \cap (A \cup \bar{B})] \cap C}_{[(B \cap A) \cup (\bar{A} \cap \bar{B})] \cap C} \} \end{aligned}$$

$$[(B \cap A) \cup (\bar{A} \cap \bar{B})] \cap C$$

$$[(\bar{A} \cap \bar{B} \cap C) \cup (\bar{B} \cap A \cap C)]$$

$$(A \Delta B) \Delta C = (A \cap \bar{B} \cap \bar{C}) \cup (\bar{A} \cap B \cap \bar{C}) \cup (\bar{A} \cap \bar{B} \cap C) \cup (A \cap B \cap C)$$

$$\begin{aligned} A \Delta (B \Delta C) &= (B \Delta C) \Delta A = (B \cap \bar{C} \cap \bar{A}) \cup (\bar{B} \cap C \cap \bar{A}) \\ &\quad \cup (\bar{B} \cap \bar{C} \cap A) \cup (B \cap C \cap A) \end{aligned}$$

donc

$$(A \Delta B) \Delta C = A \Delta (B \Delta C)$$

2-méthode

$\chi_A =$  fct caractéristique de A

$$\chi_{(A \Delta B) \Delta C} \stackrel{?}{=} \chi_{A \Delta (B \Delta C)}$$

$$\chi_{A \Delta B}(x) = (\chi_A(x) - \chi_B(x))^2$$

donc :

$$\chi_{A \Delta (B \Delta C)}(x) = (\chi_A(x) - (\chi_B(x) - \chi_C(x))^2)^2$$

= on développe

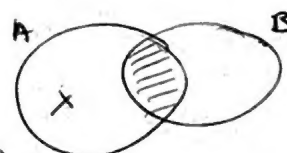
3-méthode

$$\chi : E \rightarrow \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$$

$$x \mapsto \chi(x) = \begin{cases} 0 & \text{si } x \notin A \Delta B \\ 1 & \text{si } x \in A \Delta B \end{cases}$$

Alors

$$\chi_{A \Delta B} = \chi_A + \chi_B$$



d'où  $\chi_{A \Delta (B \Delta C)} = \chi_{A \Delta B} + \chi_{B \Delta C} \Rightarrow A \Delta (B \Delta C) = (A \Delta B) \Delta C$

$$* A \Delta B = B \Delta A$$

$$* \forall A \in \mathcal{P}(E) \quad A \Delta \emptyset = A$$

$$* \forall A \quad \exists A' / A \Delta A' = \emptyset \quad \text{On prend } A' = A.$$

Remarque

$$A \mapsto \chi_A$$

$$(\mathcal{P}(E), \Delta) \rightarrow (\mathcal{P}(E, \mathbb{Z}/2\mathbb{Z}), +)$$

$$\varphi = \text{isomorphisme car } \begin{cases} * \varphi(A \Delta B) = \chi_{A \Delta B} = \chi_A + \chi_B = \varphi(A) + \varphi(B) \\ * \varphi \text{ bijective (facile)} \end{cases}$$

On peut aussi munir  $\mathbb{Z}/2\mathbb{Z}$  de la loi  $\cdot$  qui fait que  $(\mathbb{Z}/2\mathbb{Z}, +, \cdot) = \text{anneau}$ .

$$\text{Alors } (\mathbb{Z}/2\mathbb{Z})^E = \text{anneau}.$$

$$\text{Alors } \varphi : (\mathcal{P}(E), \Delta, \cap) \rightarrow ((\mathbb{Z}/2\mathbb{Z})^E, +, \cdot)$$

$$A \mapsto \chi_A$$

est un isomorphisme d'anneau.

$$\text{En effet : } \varphi(A \cap B) = \chi_{A \cap B} = \chi_A \cdot \chi_B = \varphi(A) \cdot \varphi(B)$$

3

$G = \text{groupe}$

$$(A, B) \mapsto AB = \{ a b / a \in A \text{ et } b \in B \}$$

$\alpha)$  et  $\gamma)$

$\mathcal{S}_3 = \text{groupe des permutations d'un ensemble à 3 éléments.}$

(Il y a 6 éléments, et c'est le plus petit qui soit non commutatif)

jusqu'à 5, tous commutatifs

$$\mathbb{Z}/2\mathbb{Z}$$

$$\mathbb{Z}/3\mathbb{Z}$$

$$\mathbb{Z}/5\mathbb{Z}$$

$$\rightarrow \forall G \text{ a.p.} \left. \begin{array}{l} \text{premier} \\ \text{G isom. à } \mathbb{Z}/p\mathbb{Z} \\ (\text{cf. cours}) \end{array} \right\}$$

$$\mathbb{Z}/4\mathbb{Z} \text{ isom. à } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \text{ (groupe de Klein)}$$



## Rappels

$\mathcal{I}_3$  : liste des sous-groupes

$H \subset \mathcal{I}_3$ , alors  $\#H = 2$  ou  $3$

\* si  $\text{ord}(H) = 6$ ,  $H = \mathcal{I}_3$

\* si  $\text{ordre } H = 3$   $H = \{1, (123), (132)\}$

\* si  $\text{ordre } H = 2$   $\{1, (12)\}$   $\{1, (13)\}$   $\{1, (23)\}$

\* si  $\text{ord}(H) = 1$ ,  $H = \{1\}$

(Remarque : Pro 1 :  $\text{ord}(G) = p$  premier  $\Rightarrow G$  isomorphe à  $\mathbb{Z}/p\mathbb{Z}$

Pro 2 :  $G \cong \mathbb{Z}/p\mathbb{Z} \Leftrightarrow \exists a \in G \ G = \langle a \rangle$  )

Retour au 4)

Prendons  $H = \{1, (12)\}$

$K = \{1, (13)\}$

$HK = \{1, (12), (13), (132)\}$

et  $HK \neq$  sous-groupe de  $\mathcal{I}_3$  (il sont tous répertoriés dans les rappels !)

3)  $H$  et  $K$  sous-groupes de  $G$  ;

$HK \text{ est un sous-groupe de } G \Leftrightarrow HK = KH$

Preuve :

( $\Rightarrow$ ) (Par l'absurde) supposons que  $HK$  soit un sous-groupe et que  $HK \neq KH$

$$HK \neq KH \Leftrightarrow \begin{cases} HK \not\subset KH \Leftrightarrow \exists h \exists k \forall h' \forall k' \quad hk \neq h'k' & (1) \\ \text{ou} \\ KH \not\subset HK \Leftrightarrow \exists h \exists k \forall h' \forall k' \quad kh \neq h'k' & (2) \end{cases}$$

(notations évidentes)

\* Si (1) a lieu, considérons  $(hk)^{-1}$ .

$$(hk)^{-1} \in HK \quad \text{car } HK = \text{sous-groupe}$$

$$\text{Mais alors : } \exists h' \in H \quad \exists k' \in K \quad / \quad (hk)^{-1} = h'k'$$

$$\Downarrow$$

$$hk = k'^{-1} h'^{-1}$$

faux (cf (1))

Si (2) a lieu, on considèrera  $(kh)^{-1}$  :

$$(\cancel{kh})^{-1}$$

\* Si  $\neg(1)$  a lieu.

\* Si (1) n'a pas lieu, alors  $HK \subset KH$  et (2) a lieu.

Prendons  $h$  et  $k$  définis en (2).

$$\left. \begin{array}{l} h \in HK \\ k \in HK \end{array} \right\} \Rightarrow \cancel{kh} \in HK \Rightarrow (kh)^{-1} \in HK \subset KH$$

(HK sous-groupe)

$$\text{donc : } \exists h' \in H \quad \exists k' \in K \quad / \quad (kh)^{-1} = \cancel{k'} h'$$

$$\Downarrow$$

$$kh = (h'^{-1})(k'^{-1})$$

ce qui contredit (2)

(NB : démonstration directe derrière cette feuille)

( $\Leftarrow$ )  $HK \neq \emptyset$  puisque  $e \in HK$

$\forall a \in HK \quad \forall b \in HK$  Montrons que  $ab^{-1} \in HK$

$$\left\{ \begin{array}{l} a = hk \\ b = h'k' \end{array} \right\} \Rightarrow ab^{-1} = \underbrace{hk k'^{-1} h'^{-1}}_{\in KH = HK}$$

$$ab^{-1} = \underbrace{h h_1}_{\in H} k_1 \in HK \Rightarrow ab^{-1} \in HK \text{ ouï}$$



démonstration directe  $(\Rightarrow)$

\*  $KH \subset HK$

En effet:  $\forall k \in K \quad \forall h \in H \quad (kh)^{-1} = h^{-1}k^{-1} \in HK$  sous-groupe  
 $\Downarrow$   
 $kh \in HK$

\*  $HK \subset KH$

$\forall h \in H \quad \forall k \in K \quad (hk)^{-1} \in HK (= \text{sous-groupe})$   
 $\Downarrow$   
 $\exists h' \in H \quad \exists k' \in K \quad k^{-1}h^{-1} = h'k'$   
 $kh = k'^{-1}h'^{-1} \in KH$   
donc  $HK \subset KH$

8) On suppose que  $G$  est abélien. Dans la loi  $(A, B) \mapsto AB$  est bien une loi interne dans l'ensemble des groupes.

\* Associativité

$$(AB)C = A(BC) \quad \text{oui}$$

\* élément neutre

Notons  $E = \{e\}$  Dans  $EA = AE = A$  oui  $\forall A$  groupe de  $G$ .

\* élément symétrique

Soit A • Si  $G \neq \{e\}$ , montrons que  $G$  n'admet pas de sym.

$$\exists a \in G \setminus \{e\}$$

• Si  $\forall B$  sous-groupe de  $G \quad a \in B \Rightarrow B \neq \{e\} = E$   
 $G$  n'est pas inversible.

• Si  $G = \{e\}$ ,  $\forall A$  sous-groupe de  $G$ ,  $A = G$   
et  $A = G = E$ .

• Si Alors la loi  $\times$  (qui n'a plus aucun intérêt!) est  
une loi de groupe dans l'ens. des sous-groupes  
de  $E$  (il n'y en a pas des masses)  
Conclure

Extension de la question 8)

exo || Soit  $G$  groupe et  $H$  une partie finie de  $G$   
|| Plus  $e \in H$  et  $H$  stable  $\Rightarrow H$  sous-groupe (I)

(cf tout anneau intègre fini est un corps) (II)  
lemme.

Démo: Soit  $G$  un ensemble  $\mathcal{G}$  muni d'une loi interne, associative et possédant un élément neutre.

Soit  $H$  partie finie,  $H \ni e$ , et stable.

Plus tout élément régulier de  $H$  est symétrisable

En effet:

$x \in H$  régulier

$$\beta: H \rightarrow xH$$

$$y \mapsto xy$$

\*  $\beta$  injective car  $xy = xy' \Rightarrow y = y'$

\*  $H$  fini  $\Rightarrow \beta: H \rightarrow H \Rightarrow \beta$  surjective.

Donc:  $\exists x' \in H / \beta(x') = e = xx'$  et  $x$  est inversible.

→ Application  $\tilde{\alpha}$  (I)

→ Application  $\tilde{\alpha}$  (II)

$A$  anneau int.

$$G = A \setminus \{0\}$$



⑤  $(GL(E), \circ) = \text{groupe}$   $E = K\text{-e.v.}$

Th  $\left\{ \begin{array}{l} \text{Soit } h \in GL(E) \\ h \text{ est une homothétie de } E \text{ si } \forall D \text{ droite vectorielle de } E \\ h(D) = D \end{array} \right.$

(démonstration : voir exposé cap. sur les homothéties)

Soit  $H$  l'ensemble des homothéties, et notons  $Z$  le centre de  $GL(E)$

\* On a  $H \subset Z$

\* Inversement, montrons que  $Z \subset H$

Soit  $f \in Z$

$$\forall u \in GL(E) \quad f \circ u = u \circ f$$

Soit  $D$  droite vect. de  $E$ , quelconque :

$\exists s \in GL(E)$  symétrise vect. par rapport à  $D$  // à un plan quelconque.

$$f \circ s = s \circ f$$

$$\forall x \in D \quad f(x) = s(f(x))$$

$\Uparrow \leftarrow$  Attention, si  $K$  de caractéristique  $\neq 2$   
Sinon, prendre une affinité.

$$f(x) \in D$$

$$f(D) \subset D \quad f \in GL(E) \Rightarrow f(D) = D$$

Donc  $f = \text{homothétie}$ .

④

$$\begin{aligned} \psi: GL(\mathbb{R}^2) &\xrightarrow{\psi} \{-1, 1\} \\ u &\mapsto \frac{\det u}{|\det u|} = \text{sgn}(\det u) \end{aligned}$$

$\psi$  est un morphisme de groupe, et  $\text{Ker } \psi = \{u \in GL(\mathbb{R}^2) / \det u > 0\} = GL^+(\mathbb{R}^2)$

Ainsi  $GL^+$  = sous-groupe distingué.

Remarque

$$\forall H \triangleleft G \quad \exists G' \text{ groupe tel que } \gamma: G \rightarrow G' / H = \text{Ker } \gamma$$

Preuve:

On prend  $G' = G/H$  et  $\gamma =$  surjection canonique.

⑤

Attention: la démonstration faite en algèbre utilisant les symétries par rapport à des droites est dangereuse car elle suppose que le corps sur lequel on travaille est de caractéristique différente de 2

$$E = e.v. \text{ sur } K$$

$$E = D \oplus P$$

$s =$  symétrie / à  $D$  parallèlement à  $P$ .

$$\text{Plus } \text{Inv } s = \{x \in E / s(x) = x\} = D \iff K \text{ est un corps de caractéristique } \neq 2$$

→ la démonstration se fait bien, quand  $m$ , avec une affinité de rapport  $\lambda$ .

2<sup>e</sup> solution

Montrons que  $Z \subset H$ .

$$\text{Soit } h \in Z \quad \forall u \in GL(E) \quad h \circ u = u \circ h$$

Montrons que  $h$  laisse invariant les droites.

Contraposée:  $\exists a \neq 0 \quad a \in E / (a, h(a))$  soit libre.

Soit  $F$  le plan vectoriel engendré par  $(a, h(a))$ , et  $G$  tel que  $F \oplus G = E$



Soit  $u$  telle que  $\begin{cases} u|_G = \text{Id} \\ u|_F \text{ définie par } \begin{cases} u(x) = a \\ u(h(x)) = a + h(x) \end{cases} \end{cases} \quad u \in \text{GL}(E)$

Alors  $u$  ne commute pas avec  $h$ . En effet :

$$\begin{cases} (u \circ h)(a) = u(h(a)) = a + h(a) \\ (h \circ u)(a) = h(a) \end{cases} \Rightarrow u \circ h(a) \neq h \circ u(a)$$

CQFD

⑥

Soient  $G, G'$  2 groupes, et  $\text{Hom}(G, G')$  -  $G'$  abélien

$$(\beta g)(x) = \beta(x) g(x)$$

\*  $(\text{Hom}(G, G'), \cdot) = \text{groupe?}$

$$\begin{aligned} (\beta g)(xy) &= \beta(xy) g(xy) = \beta(x) \beta(y) g(x) g(y) \\ &= \beta(x) g(x) \beta(y) g(y) \\ &= (\beta g)(x) (\beta g)(y) \end{aligned}$$

Notons  $(G', +)$ ,  $(G, \cdot)$ .  $\beta g$  est défini par :

$$(\beta g)(x) = \beta(x) g(x) + g(x)$$

Exercice

$\text{Hom}(\mathbb{Z}, G)$

Soit  $\beta \in \text{Hom}(\mathbb{Z}, G)$

$$\beta: \mathbb{Z} \rightarrow G$$

$$0 \mapsto 0$$

$$1 \mapsto \beta(1) = a \in G$$

$$\vdots$$

$$n \mapsto \beta(n) = na \quad (\text{par récurrence})$$

$$\text{où } na \text{ est défini par } \begin{cases} 0a = 0 \\ 1a = a \\ na = (n-1)a + a \end{cases}$$

Remarque On a ainsi défini la loi interne  $\mathbb{Z} \times G \rightarrow G$   
 $(n, a) \mapsto na$

qui vérifie  $\begin{cases} 1a = a \\ n(a+b) = na + nb \\ (n+m)a = na + ma \\ 0a \end{cases}$

On dit que  $G$  a une structure de module sur  $\mathbb{Z}$ .

~~Prop~~:

Réciproquement,  $\beta: \mathbb{Z} \rightarrow G$  est un homomorphisme  
 $n \mapsto na$

$$\text{Hom}(\mathbb{Z}, G) = \{ \beta: \mathbb{Z} \rightarrow G \mid \exists a \in G \ \forall n \in \mathbb{Z} \ \beta(n) = na \}$$

Remarque

● Montrer que  $\varphi: \text{Hom}(\mathbb{Z}, G) \rightarrow G$   
 $\beta \mapsto a = \beta(1)$

est un ~~hom~~ isomorphisme de groupe.

On peut ainsi identifier  $\text{Hom}(\mathbb{Z}, G)$  et  $G$ .

$$\underline{\text{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})}$$

Soit  $\beta: \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}$  ( $\beta$  morphisme)

$$\begin{aligned} 0 &\mapsto 0 \\ 1 &\mapsto \beta(1) \\ \vdots &\vdots \\ k &\mapsto k\beta(1) \\ \vdots &\vdots \\ n-1 &\mapsto (n-1)\beta(1) \end{aligned}$$

$$\text{Mais } \begin{cases} \beta(n) = n\beta(1) \\ \text{et} \\ \beta(n) = \beta(0) = 0 \end{cases}$$

$$\text{donc } n\beta(1) = 0 \Rightarrow \beta(1) = 0$$

$$\text{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) = \{0\}$$

$$\underline{\text{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})} ?$$

Cherchons  $\text{Hom}(\mathbb{Z}/n\mathbb{Z}, G)$  ( $G$  abélien)

$$\simeq \{x \in G \mid nx = 0\}$$

$G = \text{groupe abélien (noté +)}$   
 Montrer que  $\text{Hom}(\mathbb{Z}/n\mathbb{Z}, G) \simeq \overbrace{\{x \in G / nx = 0\}}^A$

Soit  $f \in \text{Hom}(\mathbb{Z}/n\mathbb{Z}, G)$

$$f: \mathbb{Z}/n\mathbb{Z} \rightarrow G$$

$$0 \mapsto 0$$

$$1 \mapsto f(1)$$

$\vdots$

$$0=n \mapsto f(n) = n f(1) = f(0) = 0 \Rightarrow n f(1) = 0.$$

$$\Rightarrow f(1) \in A$$

Considérons  $\varphi: \text{Hom}(\mathbb{Z}/n\mathbb{Z}, G) \rightarrow A$

$$f \mapsto f(1)$$

- $\varphi = \text{homomorphisme de groupes}$   $\varphi(f+g) = (f+g)(1) = \varphi(f) + \varphi(g)$
- $\varphi$  injective, car, pour  $f(1)$  fixé  $\in A$ ,  $f(p) = p f(1) \quad \forall p \in \mathbb{Z}/n\mathbb{Z} \Rightarrow f$  unique.
- $\varphi$  surjective :  $\forall x \in A \quad \exists f \in \text{Hom}(\mathbb{Z}/n\mathbb{Z}, G) \text{ morphisme de } \mathbb{Z}/n\mathbb{Z} \rightarrow G. \quad f(1) = x$   $\left\{ \begin{array}{l} \forall p \in \mathbb{Z}/n\mathbb{Z} \text{ on a } \\ f(p) = px \end{array} \right.$

② •  $\varphi$  surjective. Soit  $x \in A$ . Montrons qu'il existe  $f \in \text{Hom}(\mathbb{Z}/n\mathbb{Z}, G)$

propre telle que  $\varphi(f) = x \Leftrightarrow f(1) = x$

On définit  $f$  par :  $\forall \bar{s} \in \mathbb{Z}/n\mathbb{Z} \quad \exists k / \bar{s} = \bar{k} \quad f(\bar{s}) = kx$

Cette écriture définit bien  $f$  puisque :  $\bar{s} = \bar{k} = \bar{k}' \Rightarrow \left\{ \begin{array}{l} f(\bar{s}) = kx \\ f(\bar{s}) = k'x \end{array} \right.$

$$\text{et } k' - k = nq \Rightarrow f(\bar{s}) = kx = (k' - nq)x = k'x - q(\underbrace{nx}_0) = f(\bar{s}')$$

Cas où  $\mathbb{Z}/m\mathbb{Z} = G$

On doit chercher  $A = \{x \in \mathbb{Z}/m\mathbb{Z} / nx = 0\}$  ( $x = \text{"un" représentant de } x$ )

$$nx = 0 \Leftrightarrow m | nx \Leftrightarrow \frac{m}{\delta} \mid \frac{n}{\delta} x \quad \text{où } \Delta(m, n) = \delta$$

$$\Leftrightarrow \frac{m}{\delta} \mid x \quad (\text{cf. th. de Gauss et } \Delta(\frac{m}{\delta}, \frac{n}{\delta}) = 1)$$

$$\Leftrightarrow x \in \frac{m}{\delta} \mathbb{Z} \Leftrightarrow \exists \lambda \in \mathbb{Z} / x = \lambda \left( \frac{m}{\delta} \right)$$

d'où  $A = m'(\mathbb{Z}/m\mathbb{Z})$  où  $m = \delta m'$

$$A = m'(\mathbb{Z}/m'\delta\mathbb{Z}) \simeq \mathbb{Z}/\delta\mathbb{Z} \quad (\text{cf lemme})$$

$$\boxed{A \simeq \mathbb{Z}/\delta\mathbb{Z}}$$

lemme:  $p(\mathbb{Z}/pq\mathbb{Z}) \simeq \mathbb{Z}/q\mathbb{Z}$

$$\underbrace{p(\mathbb{Z}/pq\mathbb{Z})}_{\cong} \longrightarrow \mathbb{Z}/q\mathbb{Z}$$

$$\exists \bar{x} \in \mathbb{Z}/pq\mathbb{Z} \mid p\bar{x} = \bar{x}$$

$$\exists x \in \mathbb{Z} \mid \bar{x} = x$$

$$\begin{cases} \bar{x} \xrightarrow{\varphi} \bar{x} & (\text{classe de } x \text{ modulo } q) \\ \text{ou } \bar{x} = p\bar{x} & (\bar{x} = \text{classe de } x \text{ modulo } pq) \end{cases}$$

Peut-on définir  $\varphi$  comme cela ?

$$\bar{x} = p\bar{x}' = p\bar{x} \Rightarrow \bar{x} = \bar{x}' ?$$

$$\text{oui car } p\bar{x}' = p\bar{x} \Leftrightarrow p\bar{x}' - p\bar{x} \in \mathbb{Z}/pq\mathbb{Z}$$

$$\Leftrightarrow \bar{x}' - \bar{x} \in \mathbb{Z}/q\mathbb{Z}$$

$$\Leftrightarrow \bar{x} = \bar{x}'$$

•  $\varphi$  bien définie

•  $\varphi$  = homomorphisme bijectif

Remarque: Le lecteur vérifiera que l'isomorphisme de  $\mathbb{Z}^{\text{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})}$  vers  $\mathbb{Z}/\delta\mathbb{Z}$  (où  $\delta = \Delta(m, n)$ ) est

$$b \longmapsto \frac{1}{m'} b(i)$$

$$(\delta m' = m\mathbb{Z})$$



$$\text{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \xrightarrow{\sim} \mathbb{Z}/\Delta(m,n)\mathbb{Z}$$

Prolongement:  $\text{Aut}(\mathbb{Z}/n\mathbb{Z})$ ?

⑦.  $H = \{h \in G \mid h(x) = ax\}$

1)  $(G, \circ)$  = groupe

2)  $(G, \circ) \xrightarrow{\varphi} (\mathbb{R}^*, \times)$

$\beta = ax + b \mapsto a$

● morphisme  $\text{Ker } \varphi = \{\beta \in G \mid a=1\} = T$

donc:

•  $G/T \cong \text{Im } \varphi$  et  $\text{Im } \varphi = (\mathbb{R}^*, \times) \cong (\text{Homothéties}, \circ)$

donc  $G/T \cong (H, \circ)$  ( $H$  = ensemble des homothéties)

UNIVERSITÉ DE NICE  
INSTITUT DE MATHÉMATIQUES  
ET SCIENCES PHYSIQUES

PARC VALROSE  
06034 NICE CEDEX  
TÉL. (03) 51.91.00

MATHÉMATIQUES

M1 Algèbre et Arithmétique

## Feuille N°2

1° On munit l'ensemble  $\mathbb{R}$  de la loi de composition

$$(x, y) \mapsto \sqrt[3]{x^3 + y^3}$$

Montrer qu'on obtient ainsi un groupe isomorphe  $\bar{\alpha}(\mathbb{R}, +)$ . Plus généralement, si  $G$  est un groupe et  $f$  une bijection de  $G$  sur un ensemble  $X$ , définir un groupe isomorphe à  $G$  par  $f$  et dont l'ensemble sous-jacent soit  $X$ . Y a-t-il plusieurs solutions ?

2° Trouver tous les groupes à 1, 2, 3, 4, 5, 6, 7 éléments.

3° Soit  $G$  un groupe. Pour tout  $a \in G$ , on définit une application  $S_a: G \rightarrow G$  par  $S_a(x) = ax$  (translation à gauche d'amplitude  $a$ ). Montrer que  $a \mapsto S_a$  est un isomorphisme de  $G$  sur un groupe de permutation de  $G$ . Corollaire ?

4° Deux éléments  $x$  et  $y$  d'un groupe  $G$  sont dits conjugués s'il existe un  $s \in G$  avec  $y = sxs^{-1}$ . Montrer que la conjugaison est une relation d'équivalence dans  $G$ .

5°) Étant donné une partie  $H$  d'un groupe  $G$ , et  $s \in G$ , on note  $sHs^{-1}$  l'ensemble  $\{sa s^{-1} \mid a \in H\}$ . Montrer que si  $H$  est un sous-groupe, il en est de même de  $sHs^{-1}$ , qu'on appelle un sous-groupe conjugué de  $H$ . Le normalisateur  $N(H)$  d'un sous-groupe  $H$  de  $G$  est l'ensemble  $\{s \in G \mid sHs^{-1} = H\}$ . Montrer que  $N(H)$  est un sous-groupe (distingué?) de  $G$  et que le centre de  $G$  est un sous-groupe distingué de  $N(H)$ .

6°) Soit  $G$  un groupe, à un élément  $a \in G$  on associe l'automorphisme intérieur " $\tau_a$  de  $G$  défini par  $\tau_a(x) = axa^{-1}$ .

a) montrer que  $\tau_a \in \text{Aut } G$

b) montrer que  $a \mapsto \tau_a$  est un morphisme de groupes de  $G$  dans  $\text{Aut } G$ ; Quel est son noyau?

7°) Montrer que si deux sous-groupes  $H$  et  $K$  d'un groupe  $G$  sont d'indice fini, il en est de même de  $H \cap K$  [plonger  $G/H \times G/K$  dans  $G/H \times G/K$ ]. Montrer que si  $H \cap L$  et  $K \cap L$  sont d'indice fini dans  $G$ , il en est de même de  $H \cap K$ .

8°) Quel est l'indice de  $GL^+(\mathbb{R}^2) = \{m \in GL(\mathbb{R}^2) \mid \det m > 0\}$  dans le groupe  $GL(\mathbb{R}^2)$ .

9°) Montrer que  $\Gamma_n = \{z \in \mathbb{C} \mid z^n = 1\}$  est un sous-groupe de  $(\mathbb{C}^*, \times)$ . À quelle condition  $\Gamma_n$  est-il un sous-groupe de  $\Gamma_m$ ? Déterminer  $\Gamma_n \cap \Gamma_m$  et le sous-groupe engendré par  $\Gamma_n \cup \Gamma_m$ .

①  $\mathbb{R}/G$  définit la loi interne  $*$  sur  $\mathbb{R}$  par  $x * y = \sqrt[3]{x^3 + y^3}$

Pr :  $\varphi : (\mathbb{R}, +) \rightarrow (\mathbb{R}, *)$   
 $x \mapsto \sqrt[3]{x}$  est un morphisme surjectif pour les lois  $+$  et  $*$ .

Preuve :

- $\varphi(x+y) = \varphi(x) * \varphi(y)$
- $\varphi$  est surjective (et même bijective)

Donc  $(\mathbb{R}, *) = \text{groupe}$  (cf. rappel ci-dessous)

Rappel : Th  $\left| \begin{array}{l} G, H \text{ deux ensembles munis respectivement des lois internes } \cdot \text{ et } * \\ \text{Soit } \varphi : G \rightarrow H \text{ un morphisme surjectif pour ces lois.} \\ \text{Alors : } (G, \cdot) = \text{groupe} \Rightarrow (H, *) = \text{groupe} \end{array} \right.$

Preuve : On a  $\varphi(xy) = \varphi(x) * \varphi(y)$

- A  $(\varphi(x) * \varphi(y)) * \varphi(z) = \varphi(xyz) = \varphi(x) * (\varphi(y) * \varphi(z))$
- N  $\varphi(x) * \varphi(e) = \varphi(e) * \varphi(x) = \varphi(e)$
- S  $(\varphi(x))^{-1} = \varphi(x^{-1})$

2° Soit  $(G, \cdot)$  un groupe, et soit  $\varphi : G \rightarrow X$  bijective.

a) S'il existait une loi  $*$  donnant à  $X$  une structure de groupe rendant l'application  $\varphi$  isomorphe, on aurait forcément  $\varphi(x) * \varphi(x') = \varphi(xx')$  (1)

b) Posons, par définition :  $\forall y, y' \in X \quad y * y' = \varphi(xx')$  où  $\begin{cases} y = \varphi(x) \\ y' = \varphi(x') \end{cases}$

- On peut définir  $*$  ainsi, car  $\varphi(xx')$  est unique une fois  $x$  et  $x'$  fixés (car  $\varphi$  bijective)
- On vérifie que cette loi  $*$  ainsi définie est bien une loi de groupe sur  $X$ .

D'où le théorème (Transport des structures par une bijection)

Th  $\left| \begin{array}{l} \text{Soient } (G, \cdot) \text{ un groupe, } X \text{ un ensemble et } \varphi \text{ une bijection de } G \text{ sur } X \\ \text{Alors il existe une unique loi } * \text{ structurant } (X, *) \text{ en groupe rendant} \\ \text{l'application } \varphi \text{ isomorphe de } (G, \cdot) \text{ sur } (X, *). \\ \text{Cette loi est définie par : } \varphi(x) * \varphi(y) = \varphi(xy) \end{array} \right.$



② Trouver tous les sous-groupes à 1, 2, 3, 4, 5, 6, 7 éléments.

Soit  $G$  un groupe d'ordre  $n$ .

•  $n=1$

$$G = \{e\}$$

•  $n=2$

~~$G$  isomorphe à  $\mathbb{Z}/2\mathbb{Z}$ . En cela résulte~~

Alors  $G$  est isomorphe à  $\mathbb{Z}/2\mathbb{Z}$ .  $G$  est donc un groupe monogène.

$$G = \{e, a\} \quad \text{où } a^2 = e$$

Cela provient des théorèmes :

Th | Tout groupe d'ordre  $p$  premier est isomorphe à  $\mathbb{Z}/p\mathbb{Z}$

Th |  $G$  est un groupe monogène  $\Leftrightarrow G$  est un groupe isomorphe à  $\mathbb{Z}/n\mathbb{Z}$   
( $n \in \mathbb{N}$ )

On résout ainsi facilement les cas où  $n$  est premier :

- $n=2$   $G$  isomorphe à  $\mathbb{Z}/2\mathbb{Z}$
- $n=3$   $G$  "  $\mathbb{Z}/3\mathbb{Z}$
- $n=5$   $G$  "  $\mathbb{Z}/5\mathbb{Z}$
- $n=7$   $G$  "  $\mathbb{Z}/7\mathbb{Z}$

•  $n=4$

$$G = \{e, a, b, c\}$$

$e, a, b, c$  tous distincts entre eux

$\langle a \rangle =$  groupe d'ordre  $p$ , et  $p$  divise  $\text{ord}(G) = 4$ .

donc  $p=2$  ou  $4$  (si  $p=1$ ,  $a=e$  faux)

De 2 choses l'une :

\* Si  $\forall x \in G \ \# \langle x \rangle = 2$ , alors  $G = \{e, a, b, c\}$  où

$$\begin{aligned} a^2 &= e \\ b^2 &= e \\ c^2 &= e \end{aligned}$$

la table d'un tel groupe est :

.	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Alors  $G \sim \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  (groupe de Klein)

\* Si  $\exists x \in G$   $\text{ord}(x) = 4$ ,  $G = \{e, a, a^2, a^3\} \sim \mathbb{Z}/4\mathbb{Z}$

n=6  $G = \{e, a, b, c, d, f\}$

a)  $\exists x \in G$  /  $\text{ord}(x) = 6$ , alors  $G \sim \mathbb{Z}/6\mathbb{Z}$

b)  $\forall x \in G$   $\text{ord}(x) \neq 6$

■ Lemme | Soit  $G$ , et  $a$  tel que  $\text{ord}(a) = p$  premier  
Alors  $x \in \langle a \rangle$  et  $x \neq e \Rightarrow \langle x \rangle = \langle a \rangle$

● Preuve :

On a  $x \in \langle a \rangle \Rightarrow \langle x \rangle \subset \langle a \rangle$ , et  $\underbrace{\text{ord}(x)}_{\neq 1} \mid \text{ord}(a) = p \Rightarrow \text{ord}(x) = \text{ord}(a)$

Ainsi  $\begin{cases} \langle x \rangle \subset \langle a \rangle \\ \text{ord}(x) = \text{ord}(a) \end{cases} \Rightarrow \langle x \rangle = \langle a \rangle$

■ Pro | 1)  $G$  possède au moins un élément d'ordre 2  
2) " au moins un élément d'ordre 3

Preuve :

1) S'il n'y avait que des éléments d'ordre 3 :  $G = \{e, a, \underbrace{a^2}_b, c, \underbrace{c^2}_d, f, \dots \text{plus de place pour } f^2\}$

tous distincts (voir lemme)

2) S'il n'y avait que des éléments d'ordre 2

■ Notons  $\begin{cases} \gamma \text{ notre élément d'ordre 2} \\ \sigma \text{ notre élément d'ordre 3} \end{cases}$

	e	$\sigma$	$\sigma^2$	$\tau$	$\tau\sigma$	$\tau\sigma^2$
e	e	$\sigma$	$\sigma^2$	$\tau$	$\tau\sigma$	$\tau\sigma^2$
$\sigma$	$\sigma$	$\sigma^2$	e	$\tau\sigma^2$	$\tau$	$\tau\sigma$
$\sigma^2$	$\sigma^2$	e	$\sigma$	$\tau\sigma$	$\tau\sigma^2$	$\tau$
$\tau$	$\tau$	$\tau\sigma$	$\tau\sigma^2$	e	$\sigma$	$\sigma^2$
$\tau\sigma$	$\tau\sigma$	$\tau\sigma^2$	$\tau$	$\sigma^2$	e	$\sigma$
$\tau\sigma^2$	$\tau\sigma^2$	$\tau$	$\tau\sigma$	$\sigma$	$\sigma^2$	e

← tous distincts (le vérifier)

$\tau\sigma^2$

1 :  $\sigma\tau \neq e, \sigma, \sigma^2, \tau$ .

• Si  $\sigma\tau = \tau\sigma$ , alors  $\omega(\sigma\tau) = 6$  ( $\omega(n) = \text{ordre de } n$ ) ce qui est impossible.

On sait que  $(\sigma\tau)^6 = e$ . Reste à montrer que 6 est le p. petit nombre  $n / (\sigma\tau)^n = e$ .

$$n = 2 \text{ ou } 3. \quad * (\sigma\tau)^2 = \sigma^2\tau^2 \quad (\text{car } \sigma\tau = \tau\sigma)$$

$$= \sigma^2 \neq e$$

$$* (\sigma\tau)^3 = \tau \neq e$$

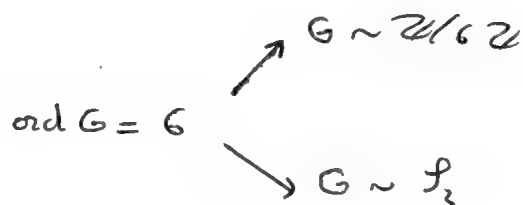
• Donc  $\boxed{\sigma\tau = \tau\sigma^2}$

On a remarqué qu'il n'y avait qu'une façon de faire la table de multiplication.

Or, je connais  $S_3$  qui est à 6 él. et qui possède 1 él. d'ordre 2 et 1 él. d'ordre 3.

3. Donc  $G \sim S_3$ .

Moralité



③

$$S_a: G \rightarrow G$$

$$x \mapsto ax$$

Soit  $S: G \rightarrow \mathcal{I}_G$

$$a \mapsto S_a$$

\*  $S_a \in \mathcal{I}_G$  car  $S_a$  est un homomorphisme

De plus  $S_a$  est bijectif, puisque:  $\forall y \in G \exists! x / ax = y$  à savoir  $x = a^{-1}y$

\*  $S$  est un homomorphisme, puisque  $\forall a, a' \in G \quad \forall x \in G \quad S_{aa'}(x) = aa'x$   
 $= a(a'x)$   
 $= S_a \circ S_{a'}(x)$

$S$  est injectif, puisque:  $\text{Ker } S = \{a \in G / \forall x \in G ax = x\} = \{e\}$

$\text{Im } S = \text{sous-groupe de } \mathcal{I}_G$

Corollaire: Tout groupe est isomorphe à un sous-groupe d'un groupe de permutations

$$G \cong \text{sous-groupe de } \mathcal{I}_G$$

⑤  $G$ ,  $A$  sous-groupe de  $G$

$$N(A) = \{ \sigma \in G / \sigma A \sigma^{-1} = \sigma_\sigma(A) = A \}$$

•  $N(A) \neq \emptyset$

•  $\sigma, \tau \in N(A) \Rightarrow \sigma_\sigma(A) = A$  ?

On a  $\sigma_\sigma(A) = \sigma_\sigma(\sigma_\tau(A)) = \sigma_\sigma(A) = A$  donc  $\sigma\tau \in N(A)$

•  $\sigma \in N(A) \Rightarrow \sigma^{-1} \in N(A)$

$N(A) = \text{sous-groupe}$ .

$N(A)$  distingué ?

Si  $A$  distingué  $N(A) = G$  puisque  $\forall x \in G \quad xAx^{-1} = A \Rightarrow x \in N(A)$   
distingué dans  $G$

Contre exemple

$$\begin{cases} G = \mathcal{I}_3 & (\text{plus petit sous-groupe non commutatif}) \\ A = \{1, \tau\} & (\tau = \text{transposition}) \end{cases}$$

$A$  est bien un sous-groupe non distingué car, si  $\sigma = \text{autre transposition}$ ,  $\sigma\tau\sigma^{-1} \neq \tau$

et  $\sigma\tau\sigma^{-1} \neq \tau$  car autrement  $\sigma\tau = \tau\sigma \Rightarrow \exists$  sous le sous-groupe engendré <sup>par</sup>  $\{\sigma$  et  $\tau\}$  serait  $\{1, \sigma, \tau, \sigma\tau\}$  d'ordre 4, qui ne divise pas 6 !

$$\sigma \in N(A) \Leftrightarrow \begin{cases} \sigma \tau \sigma^{-1} = \tau \\ \sigma \tau \sigma^{-1} = \tau \end{cases}$$

$$\text{On a } \underbrace{A \subset N(A)}_{\text{ordre 2}} \subset \underbrace{F_3}_{\text{ordre } n} \Rightarrow 2 \mid n \text{ et } n \mid 6 \Rightarrow n = 2 \text{ ou } 6$$

Or  $n \neq 6$ , sinon  $N(A) = G \Rightarrow A \trianglelefteq G$  faux.

Remarque : Règle de calcul.

$$\left[ \begin{array}{l} \sigma \tau \sigma^{-1} \text{ et } \tau = (a_0, \dots, a_n) \\ \text{Alors } \sigma \tau \sigma^{-1} = (\sigma(a_0), \dots, \sigma(a_n)) \end{array} \right.$$

$$\text{On montre que } \begin{cases} \sigma \mid_{\{\sigma(a_0), \dots, \sigma(a_n)\}} = \sigma \tau \sigma^{-1} \mid_{\{\sigma(a_0), \dots, \sigma(a_n)\}} \\ \sigma \mid_{C\{\sigma(a_0), \dots, \sigma(a_n)\}} = \text{Id} \end{cases}$$

$$\underline{Z \trianglelefteq N(A)}$$

1-démonstration

$$Z = \text{centre de } A = \{z \in A \mid \forall x \in A \quad zx = xz\}$$

$Z$  = sous-groupe distingué de  $N(A)$  car :

- $Z \subset N(A)$  trivial
- $Z$  = sous-groupe trivial
- $Z$  distingué dans  $N(A)$  ?

$$\forall z \in Z \quad \forall \sigma \in N(A) \quad \sigma z \sigma^{-1} \in Z ?$$

$$\text{On a : } \forall x \in A \quad \sigma z \sigma^{-1} x = \sigma z x \sigma^{-1} \quad \text{ou} \quad \sigma^{-1} x \sigma = x' \in A \quad (\text{car } \sigma \in N(A))$$

$$= \sigma x' z \sigma^{-1} \quad \text{car } x' z = z x' \quad (x' \in A \quad z \in Z(A))$$

$$\sigma z \sigma^{-1} x = x'' \sigma z \sigma^{-1} \quad \text{ou} \quad \sigma x' \sigma^{-1} = x'' \in A \quad (\text{car } \sigma \in N(A))$$

$$\text{Donc : } x'' = \sigma x' \sigma^{-1} = \sigma (\sigma^{-1} x \sigma) \sigma^{-1} = x$$

$$\text{d'où : } \forall x \in A \quad (\sigma z \sigma^{-1}) x = x (\sigma z \sigma^{-1}) \Leftrightarrow \sigma z \sigma^{-1} \in Z$$

Q.E.D.



## 2<sup>e</sup> démonstration

$$\left. \begin{array}{l} G \text{ a } Z(A) \trianglelefteq A \\ A \subset N(A) \text{ et } A \trianglelefteq N(A) \end{array} \right\} \Rightarrow Z(A) \trianglelefteq N(A)$$

où :  $H \trianglelefteq G \Leftrightarrow \forall u \in \text{Aut}(G) \quad u(H) \subset H$   
cf théorème  $H \trianglelefteq G \trianglelefteq L \Rightarrow H \trianglelefteq L$

Remarque : "le normalisateur  $N(A)$  est le plus grand sous-groupe de  $G$  dans lequel  $A$  est distingué".

Preuve :  $A \trianglelefteq H \subset G \Rightarrow H \subset N(A)$



$$\forall t \in H \quad \sigma_t(A) = A \Rightarrow \forall t \in H \quad t \in N(A)$$

⑦  $H \subset G$

L'indice du groupe  $H$  dans  $G$  est, par définition

$$[G : H] = \text{Card}(G/H) = \text{Card}(H \backslash G) \quad (1)$$

[1) : En effet  $\exists$  bijection  $G/H \rightarrow H \backslash G$   
 $xH \mapsto Hx^{-1}$

car :  $xH = x'H \Leftrightarrow Hx^{-1} = Hx'^{-1}$



$$x^{-1}x' \in H \Leftrightarrow x'^{-1}x \in H \quad ]$$

## exercice

a)  $G/H$  et  $G/K$  binis  $\Rightarrow G/H \cap K$  bini

Soit  $\varphi: G/H \cap K \rightarrow G/H \times G/K$

$$(H \cap K)x \mapsto Hx \times Kx$$

Existe ?  $(H \cap K)x = (H \cap K)x'$

$$\begin{aligned} &\Leftrightarrow \\ &xx'^{-1} \in H \cap K \\ &\Leftrightarrow \end{aligned}$$

$$\begin{cases} xx'^{-1} \in H \\ \text{et} \\ xx'^{-1} \in K \end{cases} \Leftrightarrow \begin{cases} Hx = Hx' \\ Kx = Kx' \end{cases}$$

ce qui montre, d'un coup, que  $\varphi$  est définie et est injective

CQFD

b)  $G/H \cap L$  fini et  $G/K \cap L$  fini  $\Rightarrow G/H \cap K$  fini.

d'après (a), on a  $G/H \cap L$  fini et  $G/K \cap L$  fini  $\Rightarrow G/H \cap K \cap L$  fini.

Or  $\varphi: G/H \cap K \cap L \xrightarrow{\text{surj.}} G/H \cap K$  est définie et surjective.

$$(H \cap K \cap L)x \mapsto (H \cap K)x$$

définie:  $(H \cap K \cap L)x = (H \cap K \cap L)x' \Leftrightarrow xx'^{-1} \in H \cap K \cap L \subset H \cap K$   
 $\Rightarrow (H \cap K)x = (H \cap K)x'$

surjectivité:  $\exists x \in G / \exists = (H \cap K)x \Rightarrow \exists = \varphi(x(H \cap K \cap L))$

donc  $G/H \cap K$  fini.

⑧

On sait que  $GL^+(\mathbb{R}^2) = \{m \in GL(\mathbb{R}^2) / \det m > 0\}$  est un sous-groupe distingué de  $GL(\mathbb{R}^2)$  (cf.  $\varphi: GL(\mathbb{R}^2) \rightarrow \{-1, 1\}$ )  
 $m \mapsto \frac{\det m}{|\det m|}$

ord( $GL(\mathbb{R}^2)/GL^+(\mathbb{R}^2)$ ) ?

$$\begin{array}{ccc} GL(\mathbb{R}^2) & \xrightarrow{\varphi} & \{-1, 1\} \\ \pi \downarrow & \nearrow \tilde{\varphi} = \text{isomorphisme} & \\ GL(\mathbb{R}^2) & & \\ \downarrow & & \\ GL^+(\mathbb{R}^2) & & \end{array}$$

car  $\ker \varphi = GL^+(\mathbb{R}^2)$

Donc  $\text{ord}(GL(\mathbb{R}^2)/GL^+(\mathbb{R}^2)) = 2$  (cf. orientation d'un e.v.)

⑨  $n \neq 0 \quad \Gamma_n = \{z \in \mathbb{C} / z^n = 1\}$

$\Gamma_n = \text{sous-groupe de } \mathbb{C}^* \text{ (c'est le noyau de } (\mathbb{C}^*, x) \rightarrow (\mathbb{C}^*, x) \text{)}$   
 $z \mapsto z^n$

(NB:  $\Gamma_n$  isomorphe à  $\mathbb{Z}/n\mathbb{Z}$  car  $\mathbb{Z}/n\mathbb{Z} \rightarrow \Gamma_n$   
 $k \mapsto e^{i \frac{2\pi k}{n}}$

Pro  $\Gamma_n \subset \Gamma_m \Leftrightarrow n|m$

( $\Rightarrow$ )  $\Gamma_n = \text{sous-groupe de } \Gamma_m \Rightarrow n|m$

( $\Leftarrow$ )  $m=nq \Rightarrow z^n = 1 \Rightarrow z^m = 1$

Pro  $\Gamma_n \cap \Gamma_m = \Gamma_{\Delta(m,n)}$

En effet  $\Gamma_n \cap \Gamma_m = \{z \in \mathbb{C}^* / z^n = z^m = 1\} \rightarrow \text{si } n|m, \Gamma_n \cap \Gamma_m = \Gamma_n$   
 (par ex.  $n \leq m$ )  $\rightarrow \text{si } n \nmid m$

$m = nq + r \quad r < n$   
 $z^n = z^{nq+r} = 1 \Leftrightarrow z^n = z^r = 1$

On obtient ainsi une suite strictement  $\searrow$  dans  $\mathbb{N}$  qui converge

donc donc  $\begin{cases} m = nq + r \\ n = r q_1 + r_1 \\ \dots \\ r_{k+1} = r_{k+2} q_{k+3} + 0 \end{cases}$  et  $\Delta(m,n) = r_{k+2}$   
 $\Gamma_n \cap \Gamma_m = \Gamma_{r_{k+2}}$   
 dernier reste non nul.

$\leftarrow$  (algorithme d'Euclide)

$\begin{cases} \text{si } r|n & \cap = \Gamma_n \\ \text{sinon, on continue} \end{cases}$

$\Gamma_n \cap \Gamma_m = \Gamma_{\Delta(m,n)}$

Remarque : autre démonstration.

Si  $G = \text{sous-groupe fini de } \mathbb{C}^*$ , alors  $G = \Gamma_n$  où  $n = \# G$

(voir th. cours)

Preuve: Soit  $z \in G \quad z^n = 1 \Rightarrow G \subset \Gamma_n$   
 ou  $\# \Gamma_n = n \Rightarrow \Gamma_n = G$

$z \in \Gamma_n \cap \Gamma_m \Leftrightarrow (z^d)^{n'} = (z^d)^{m'} = 1 \quad \text{ou} \quad \Delta(m', n') = 1$   
 $\Leftrightarrow z^d \in \Gamma_{n'} \cap \Gamma_{m'} \quad \begin{cases} m = m'd \\ n = n'd \end{cases}$

(NB) Corps des quaternions  $\mathbb{H}$

1-définition  $1, i, j, k$  base de  $\mathbb{H}$

$x$  dans  $\mathbb{Q}$  1 neutre  $i^2 = j^2 = k^2 = -1$ ;  $ij = k, ki = j$ ;  $jk = i$

$a + bi + cj + dk$   $\begin{matrix} -ji & -ik & -kj \end{matrix}$

2-façon géométrique ( $\wedge$ )

C'est le plus petit corps non commutatif

$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H}$  (1950): il n'y a pas de corps entre, ni après.

Suite:  $\nexists z^d \in \Gamma_n \cap \Gamma_{m'} (1)$

$\Gamma_n \cap \Gamma_{m'} = \text{sous-groupe fini de } \mathbb{C}^* \Rightarrow \exists \Gamma_n \cap \Gamma_{m'} = \Gamma_{d'}$

et  $\left. \begin{matrix} \Gamma_{d'} \subset \Gamma_n \Rightarrow d' | n \\ \Gamma_{d'} \subset \Gamma_{m'} \Rightarrow d' | m' \end{matrix} \right\} \Rightarrow d' = 1$   
 $d(m, n') = 1$

(1)  $\Leftrightarrow$  donc  $z^d \in \Gamma_{d'} = \Gamma_1$

$$(z^d)^{-1} = 1 = z^d$$

$$\Downarrow$$

$$\Gamma_n \cap \Gamma_m \subset \Gamma_d$$

La réciproque est vraie car  $d | n$  et  $d | m \Rightarrow \Gamma_d \subset \Gamma_n \cap \Gamma_m$

autre démonstration

$$\begin{matrix} \mathbb{N}^* & \xrightarrow{\eta} & \{\text{groupes finis de } \mathbb{C}^*\} \\ n & \mapsto & \Gamma_n \end{matrix}$$

• elle est bijective (réciproque:  $\# G \leftarrow G$ )

•  $(\mathbb{N}^*, |)$   $\{\eta, \subset\}$   
 $\uparrow$   $\uparrow$   
 adhé  $\uparrow$  adhé

l'application est croissante car  $n | m \Rightarrow \Gamma_n \subset \Gamma_m$

C'est un isomorphisme pour la relation d'ordre ( $\Leftrightarrow$  bijection croissante)

$$\mathbb{N}^* \longrightarrow \eta$$

$n, m$

$\Gamma_n, \Gamma_m$

$$d = \Delta(m, n)$$

$\Gamma_d =$  le plus grand sous-groupe  
commun à  $\Gamma_m$  et  $\Gamma_n$

$\Downarrow$

$$\Gamma_d = \Gamma_m \cap \Gamma_n$$

$$b) \langle \Gamma_n \cup \Gamma_m \rangle$$

$$(\mathbb{N}^*, 1) \longrightarrow (\eta, c)$$

$n, m$

$p =$  le plus petit multiple  
commun à  $n$  et  $m$

$\langle \Gamma_n \cup \Gamma_m \rangle =$  le plus petit sous-groupe de  $\mathbb{Q}^*$   
contenant  $\Gamma_n \cup \Gamma_m$ .

on traduit

$$\left. \begin{array}{l} \Gamma_n \subset \Gamma_{nn} \\ \Gamma_m \subset \Gamma_{mn} \end{array} \right\} \Rightarrow \langle \Gamma_n \cup \Gamma_m \rangle = \text{sous-groupe fini.}$$

$$\text{donc } \langle \Gamma_n \cup \Gamma_m \rangle = \Gamma_p$$



## Feuille d'exercices N°3

- x 1° Montrer que  $S_4$  possède un sous-groupe distingué isomorphe au groupe de Klein.
- x 2° Montrer que pour deux sous-groupes  $H$  et  $G$  de  $\Gamma$ ,  $H \triangleleft \Gamma$  et  $G \triangleleft H$  n'implique pas  $G \triangleleft \Gamma$ .
- x 3° Montrer qu'un sous-groupe d'indice deux est distingué.
- x 4° Quels sont les sous-groupes maximaux de  $\mathbb{Z}/n\mathbb{Z}$ ?
- x 5° Soient  $a$  et  $b$  dans  $\mathbb{Z}$ .  
Si  $(a, b) = 1$ , montrer qu'il existe  $u, v \in \mathbb{Z}$  vérifiant  $ua + vb = 1$  avec  $|u| < |b|$  et  $|v| < |a|$ . Unicité?
- x 6° Quels sont les éléments d'ordre 2 de  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ ?  
Quels sont ceux d'ordre 4? Trouver tous les automorphismes de  $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$  [pour  $a, b \in G$  avec  $\omega(a) = 2, \omega(b) = 4$ , l'appliquer  
tion  $f: G \rightarrow G$  définie par  $f(x, y) = xa + yb$  est linéaire]
- x 7° Déterminer  $\text{Aut}(S_3), \text{Aut}(\mathcal{H})$ , muni  
 $S_3 \times \mathcal{H}$  d'une structure de groupe isomorphe à  $S_4$ .

x 87 Déterminer le groupe  $\text{Aut}(\mathbb{Z}/n\mathbb{Z})$  [préciser pour  $n = 2, 3, 4, 5$   
7, 8, 13, 15, 21  
24]

x 97 Montrer, de deux façons différents que  $\frac{(2a)! (2b)!}{a! b! (a+b)!}$  est un entier.

x 107 Si  $a_1, \dots, a_n \in \mathbb{Z}$  vérifient  $\sum_{i=1}^n a_i = 0$ , montrer que pour tout nombre premier  $p$ ,  $\min \{v_p(a_i) \mid 1 \leq i \leq n\}$  est atteint au moins deux fois. Montrer que  $S_n = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n}$  n'est jamais entier pour  $n > 1$  [Observer que  $v_2(x)$  pour  $x = 1, 2, \dots, n$  atteint une fois son maximum]

AS 117 Les suites  $[a_n], [b_n], n \in \mathbb{N}$  représentent\* une fois et une seule les entiers (traduisez!) si et seulement si  $a, b \notin \mathbb{Q}, a, b > 0$  et  $\frac{1}{a} + \frac{1}{b} = 1$ .

d'où  $H \cong H'$   
x 137 Trouver un groupe  $G$ , deux sous-groupes  $H$  et  $H'$  de  $G$ , isomorphes, et tels que  $G/H$  et  $G/H'$  non isomorphes.

$G/H \cong G/H'$   
ne pas confondre  $\cong$  et  $=$ !  
x 147 Montrer que le nombre de diviseurs de  $a \in \mathbb{N}$  est impair si et seulement si  $a$  est un carré.

4. x 11. 78

\* c.à.d.  $a, b \in \mathbb{R} \quad (a_n), (b_n) \quad \forall x \in \mathbb{R} \quad \exists ! n$

Existence

$$\textcircled{5} \Delta(a, b) = 1$$

$$\exists u_0, v_0 / au_0 + bv_0 = 1 \quad (\text{Equation de Bezout})$$

On peut résoudre l'Equation (1) à inconnues  $u, v \in \mathbb{Z}$ :

$$(1) \quad au + bv = 1$$

$$(1) \Leftrightarrow \exists q \in \mathbb{Z} \begin{cases} u = u_0 + bq \\ v = v_0 - aq \end{cases}$$

On veut trouver  $q \in \mathbb{Z}$  tel que  $\begin{cases} |u| < |b| \\ \text{et} \\ |v| < |a| \end{cases} \Leftrightarrow \begin{cases} |u_0 + bq| < |b| \\ |v_0 - aq| < |a| \end{cases}$

$$n : \begin{cases} \exists! q \in \mathbb{Z} \quad \exists! n \in \mathbb{Z} & u_0 = (-b)q + n & \text{où } |n| < \frac{|b|}{2} \end{cases} \quad (2)$$

$$\begin{cases} \exists! q' \in \mathbb{Z} \quad \exists! n' \in \mathbb{Z} & v_0 = aq' + n' & \text{où } |n'| < \frac{|a|}{2} \end{cases} \quad (3)$$

Preons  $n = u$  et  $n' = v$ . Pour que  $(u, v)$  soit solution de (1), il suffira que  $q = q'$ .

Montrons donc que  $q = q'$ .

$$au_0 + bv_0 = 1 \Leftrightarrow a(-bq + u) + b(aq' + v) = 1$$

$$\Leftrightarrow au + bv + ab(q' - q) = 1$$

$$\Leftrightarrow au + bv = 1 - ab(q' - q) \quad (4)$$

$$\begin{aligned} \text{Si } q \neq q' \quad |(q' - q)| \geq 1 &\Rightarrow \underbrace{|au + bv|}_{< |ab|} = \underbrace{|1 - ab(q' - q)|}_{\geq |1 - |ab||} \\ &\geq |1 - |ab|| \\ &\geq |ab(q' - q)| - 1 \\ &\geq |ab| - 1 \\ &> |ab| \end{aligned}$$

d'où la contradiction.

$$\text{Donc } q = q' \Rightarrow \begin{cases} u = u_0 + bq \\ v = v_0 - aq \end{cases} (u, v) \text{ sol. de (1) et } \begin{cases} |u| < |b| \\ |v| < |a| \end{cases} \quad \text{CQFD}$$

$$(5) \exists u_0, v_0 / au_0 + bv_0 = 1 \quad \underline{a, b \neq \pm 1} \quad (\Delta(a, b) = 1)$$

$$u_0 = bq + u \quad 0 < u < |b|$$

$$\text{d'où} \quad a(bq + u) + bv_0 = 1 \Leftrightarrow au + b(\underbrace{v_0 + aq}_r) = 1$$

$$\text{A-t'on } |v_0 + aq| < |a| ?$$

$$|v_0 + aq| < |a| \Leftrightarrow |1 - au| < |ab|$$

$$\text{mais en } |au| + 1 < |ab| + 1$$

$$\text{donc } |v| \leq \frac{1}{|b|} + |a| \text{ dans } \mathbb{Z}, \text{ donc } |v| \leq |a|$$

et  $|v| \neq |a|$  sinon ...

donc  $v < |a|$

Pas unicité

$$\begin{aligned} 2 \cdot 3 + (-1) \cdot 5 &= 1 \\ (-3) \cdot 3 + 2 \cdot 5 &= 1 \end{aligned}$$

Remarque : Pour les polynômes, il y a unicité, alors qu'il n'y avait pas unicité dans  $\mathbb{Z}$  !

$$\Delta(P, Q) = 1 \quad \exists U, V / UP + VQ = 1 \quad \text{et} \quad \begin{cases} \deg U < \deg Q \\ \deg V < \deg P \end{cases}$$

$$\begin{cases} U'P + V'Q = 1 \\ UP + VQ = 1 \end{cases} \Leftrightarrow (U' - U)P = (V - V')Q$$

après le théorème de Gauss :  $Q \mid U' - U$  et  $\deg(U' - U) < \deg Q \Rightarrow U' = U$ .

cqfd

(Cela provient de : on peut faire augmenter la valeur absolue de  $a - b$ , alors qu'on ne peut pas faire augmenter le degré de  $P - Q$ .)

$$(6) \quad G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \text{ n'est pas cyclique car } \Delta(2, 4) \neq 1.$$

$$\omega(\bar{a}, \bar{b}) = \text{ppcm}(\omega(\bar{a}), \omega(\bar{b})) \text{ d'où :}$$

$$(\bar{0}, \bar{0}) \text{ d'ordre } 1 \quad (\bar{1}, \bar{0}) \text{ d'ordre } 2$$

$$(\bar{0}, \bar{1}) \quad " \quad 4 \quad (\bar{1}, \bar{1}) \quad " \quad 4$$

$$(\bar{0}, \bar{2}) \quad " \quad 2 \quad (\bar{1}, \bar{2}) \quad " \quad 2$$

$$(\bar{0}, \bar{3}) \quad " \quad 4 \quad (\bar{1}, \bar{3}) \quad " \quad 4$$

Soir

$$f: G \rightarrow G$$

$$(x, y) \mapsto xa + yb \quad \text{ou} \quad \begin{cases} \omega(a) = 2 \\ \omega(b) = 4 \end{cases}$$

$f$  est bien définie, car :

$$\text{Si } \begin{matrix} x = x' \\ y = y' \end{matrix}, \text{ on a : } xa + yb = x'a + y'b$$

$$\text{puisque } \underbrace{(x-x')}_{2k} a = \underbrace{(y-y')}_{4q} b$$
$$\begin{array}{ccc} & \parallel & \parallel \\ & 0 & 0 \end{array}$$

$f$  est un automorphisme de  $G$  car : \*  $f$  est un morphisme

\*  $f$  bijective? Pas tout.

① Soit  $K = \{1, (12)(34), (13)(24), (23)(14)\}$

$K$  possède tous les éléments de  $\mathcal{S}_4$  décomposables en produit de 2 cycles de longueur 2, puisqu'il y a 6 transpositions distinctes de  $\mathcal{S}_4$ . C'est un sous-groupe de  $\mathcal{S}_4 \Rightarrow \cong$  au groupe de Klein.

Montrons que  $K \triangleleft A_4$  et que  $K \triangleleft \mathcal{S}_4$

1°/  $K \triangleleft A_4$

•  $K$  est bien un sous-groupe de  $A_4$ , puisque  $\text{Sgn } \sigma = 1 \ (\forall \sigma \in K)$

•  $\forall \sigma \in K \ \forall \tau \in A_4 \quad \tau \sigma \tau^{-1} \in K$

En effet,  $\tau \sigma \tau^{-1} = \text{conjugué de } \sigma \Leftrightarrow \tau \sigma \tau^{-1} \text{ et } \sigma \text{ sont décomposables en cycles de même longueur 2-2}$

$$\Downarrow$$

$$\tau \sigma \tau^{-1} \in K$$

2°/  $K \triangleleft \mathcal{S}_4$

•  $K = \text{sous-groupe de } \mathcal{S}_4$ , isomorphe au groupe  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

•  $\forall \sigma \in K \ \forall \tau \in \mathcal{S}_4 \quad \tau \sigma \tau^{-1} \in K$  (même démonstration qu'en 1°), donc  $K$  distingué dans  $\mathcal{S}_4$

② Contre-exemple : (la relation de distinction n'est pas transitive.)

$$A \triangleleft B \triangleleft C \not\Rightarrow A \triangleleft C$$

Soient  $\mathcal{S}_4$ ,  $K = \{1, (12)(34), (13)(24), (24)(13)\}$  et  $A = \{1, (12)(34)\}$

$\begin{cases} A \subset K, K \text{ commutatif car } \cong \text{groupe de Klein} \\ A = \text{sous-groupe de } K \end{cases} \Rightarrow A \triangleleft K$

b) On a vu au ① que  $K \triangleleft \mathcal{S}_4$

c) Montrons que, pourtant,  $A$  n'est pas distingué dans  $\mathcal{S}_4$ .

Nous avons :  $(132) \underbrace{[(12)(34)]}_{\in A} (123) = (24) \notin A$

(QFD)



$$\textcircled{3} \text{ ad } G/H=2 \Rightarrow G/H = \{H, G \setminus H\}$$

$$\forall x \notin H \quad Hx = G \setminus H \quad (1)$$

$$\text{ad } G/H = \text{ad}_H G \Rightarrow H \setminus G = \{H, G \setminus H\}$$

$$\forall x \notin H \quad xH = G \setminus H \quad (2)$$

$$(1) \text{ et } (2) \Rightarrow \forall x \notin H \quad xH = Hx$$

### Exercice Suppl

$$m \geq 1$$

Alors  $\{n \in \mathbb{N}^* / \varphi(n) = m\}$  est bornée. (donc fini)

$$n = \prod p_i^{n_i} \quad n_i > 0$$

$$\varphi(n) = \prod p_i^{n_i-1} (p_i-1) = n \prod \left(1 - \frac{1}{p_i}\right)$$

on a:  $\frac{1}{x} \cdot \frac{\prod \frac{p_i-1}{p_i}}{\varphi(n)}$  en fonction de  $\frac{1}{\varphi(n)}$  ?

$$\varphi(n) \prod \frac{p_i-1}{p_i} = \prod \frac{p_i-1}{p_i} p_i^{n_i-1} (p_i-1) = \prod (p_i-1)^2 p_i^{n_i-2}$$

Que dire de  $(p-1)^2 p^{n-2} \stackrel{?}{=} \delta$  ?

$$n \geq 2 \Rightarrow \delta = (p-1)^2 p^{n-2} \geq 1$$

$$n=1 \Rightarrow \delta = (p-1)^2 \frac{1}{p} = p-2 + \frac{1}{p}$$

$$\text{si } p \geq 3 \quad \delta \geq 1$$

$$\text{si } p=2 \quad \delta = \frac{1}{2}$$

Donc:  ~~$\forall p$~~

$$\left[ \begin{array}{l} \forall n \geq 1 \\ \left\{ \begin{array}{ll} \forall p > 2 & \delta \geq 1 \\ p=2 & \delta \geq \frac{1}{2} \end{array} \right. \end{array} \right.$$

Donc  $\prod_{i=1}^n (p_i - 1) \geq \frac{1}{2} \Rightarrow \prod_{i=1}^n \frac{p_i - 1}{p_i} \geq \frac{1}{2^{\varphi(n)}} \Rightarrow \frac{\varphi(n)}{n} \geq \frac{1}{2^{\varphi(n)}}$

d'où  $n \leq 2 (\varphi(n))^2$

Rappel : Sous-groupes de  $\mathbb{Z}/n\mathbb{Z}$

$\pi : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$

Soit  $G$  un sous-groupe de  $\mathbb{Z}/n\mathbb{Z}$ , alors  $\pi^{-1}(G)$  est un sous-groupe de  $\mathbb{Z}$  contenant

$\pi^{-1}(0) = n\mathbb{Z}$ . Posons  $\pi^{-1}(G) = d\mathbb{Z} \supset n\mathbb{Z}$  (\*)

Nous aurons  $\pi(d\mathbb{Z}) = G$  (car  $\pi$  est surjective)

Pro | Il existe une bijection entre les diviseurs de  $n$  ( $d$ ) et les sous-groupes de  $\mathbb{Z}/n\mathbb{Z}$  ( $\pi(d\mathbb{Z})$ )

Preuve :

- A chaque diviseur  $d$  de  $n$  on fait correspondre le sous-groupe  $\pi(d\mathbb{Z}) \subset \mathbb{Z}/n\mathbb{Z}$ .
- Cette application est surjective par construction (cf (\*))
- Injectivité?

Montrons que  $\left. \begin{array}{l} \pi(d\mathbb{Z}) = \pi(d'\mathbb{Z}) \\ d|n \text{ et } d'|n \end{array} \right\} \Rightarrow d = d'$

Nous avons :  $\pi(d) \in \pi(d'\mathbb{Z}) \Leftrightarrow \exists a \in \mathbb{Z} / d - d'a \in n\mathbb{Z}$   
 $\Leftrightarrow \exists a \in \mathbb{Z} / n | (d - d'a)$   
 $\Leftrightarrow \exists b \exists a / d - d'a = bn$

or  $d'|n \Rightarrow d' | d$   
 de m :  $d | d'$  }  $\Rightarrow d = d'$  oui

Remarque  $\pi(d\mathbb{Z}) = \{ \bar{x} \in \mathbb{Z}/n\mathbb{Z} / \exists x \in \mathbb{Z} \quad \bar{x} = d\bar{x} \} = d(\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/\frac{n}{d}\mathbb{Z}$

④ Sous-groupes maximaux de  $\mathbb{Z}/n\mathbb{Z}$

$G \subset \mathbb{Z}/n\mathbb{Z}$  est maximal  $\Leftrightarrow \left\{ \begin{array}{l} G \subset H \subset \mathbb{Z}/n\mathbb{Z} \\ \Downarrow \\ H = G \text{ ou } H = \mathbb{Z}/n\mathbb{Z} \end{array} \right.$

#### 1-méthode

Soit  $G$  maximal, alors  $\exists ! d \mid n$  et  $G = \pi(d\mathbb{Z})$

Soit  $H / G \subset \mathbb{Z}/n\mathbb{Z}$   $\exists ! d' \mid n$  /  $H = \pi(d'\mathbb{Z})$

$$\text{et } \pi(d'\mathbb{Z}) \supset \pi(d\mathbb{Z}) \Rightarrow \underbrace{\pi^{-1}(\pi(d'\mathbb{Z}))}_{= d'\mathbb{Z}} \supset \underbrace{\pi^{-1}(\pi(d\mathbb{Z}))}_{= d\mathbb{Z}} \quad (\text{cf. lemme})$$

Lemme : on a toujours  $d\mathbb{Z} \subset \pi^{-1}(\pi(d\mathbb{Z}))$

Montrons l'inclusion inverse. Soit  $x \in \pi^{-1}(\pi(d\mathbb{Z}))$ ,

$$\pi(x) \in \pi(d\mathbb{Z}) \Leftrightarrow \exists y \in d\mathbb{Z} \quad \pi(x) = \pi(y)$$

$$\Leftrightarrow x - y \in \underbrace{n\mathbb{Z}}_{\text{noyau de } \pi} \subset d\mathbb{Z} \Rightarrow x \in d\mathbb{Z}$$

$$\text{Ainsi : } \pi(d'\mathbb{Z}) \supset \pi(d\mathbb{Z}) \Leftrightarrow d'\mathbb{Z} \supset d\mathbb{Z}$$

$$\pi(d'\mathbb{Z}) \supset \pi(d\mathbb{Z}) \Leftrightarrow d' \mid d$$



$$H = G \text{ ou } \mathbb{Z}/n\mathbb{Z}$$

c.à.d :

$$\pi(d'\mathbb{Z}) = \pi(d\mathbb{Z})$$

ou

$$\pi(d'\mathbb{Z}) = \pi(\mathbb{Z})$$

$$\Leftrightarrow \begin{cases} d' = d \\ \text{ou} \\ d' = 1 \end{cases}$$

$$\text{Ainsi } \{ G \text{ maximal } \mid \pi(d\mathbb{Z}) = G \} \Leftrightarrow \{ \forall d' \mid d \Rightarrow d' = d \text{ ou } d' = 1 \}$$



$d$  premier

cd

$$G \text{ maximal} \Leftrightarrow d = \text{diviseur premier de } n$$

#### 2-méthode (c'est la mienne!)

Soit  $G \subset \mathbb{Z}/n\mathbb{Z}$ .

$$G \text{ maximal} \Leftrightarrow \nexists G' \text{ sous-groupe strict de } \mathbb{Z}/n\mathbb{Z} \mid G \subsetneq G' \subset \mathbb{Z}/n\mathbb{Z}$$

$$\Leftrightarrow \nexists d' \neq d \text{ et } n \text{ tel que } d \mid d' \text{ et } d' \mid n \quad (1)$$

$$\text{Soit } n = p_1^{\alpha_1} \dots p_k^{\alpha_k}.$$

Pro  $G \subset \mathbb{Z}/n\mathbb{Z}$   
 $G$  maximal, d'ordre  $d \Leftrightarrow \exists i / d = p_1^{\alpha_1} \dots p_{i-1}^{\alpha_{i-1}} p_i^{\alpha_i-1} p_{i+1}^{\alpha_{i+1}} \dots p_k^{\alpha_k}$

( $\Leftarrow$ ) Prenons  $d = p_1^{\alpha_1-1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$   
 Si  $d \nmid n$ , alors  $d' = p_1^{\beta_1} \dots p_k^{\beta_k}$  où  $\beta_i \leq \alpha_i$  ( $\forall i$ )  
 Si  $d \mid d'$ , alors  $\begin{cases} \alpha_1-1 \leq \beta_1 \\ \alpha_i \leq \beta_i \quad i \in [2, k] \end{cases}$  d'où  $\begin{cases} \alpha_1-1 \leq \beta_1 \leq \alpha_1 \\ \alpha_i = \beta_i \quad i \in [2, k] \end{cases}$

c.à.d.  $d = d' \mid n \Rightarrow G$  maximal

( $\Rightarrow$ ) Contraposée.

Si  $d = p_1^{\delta_1} \dots p_k^{\delta_k}$  où  $\delta_1 + \dots + \delta_k \leq (\alpha_1 + \dots + \alpha_k) - 2$

Alors:  $\exists i \in [1, k] / \delta_i + 1 \leq \alpha_i$

et  $d' = p_1^{\delta_1} \dots p_i^{\delta_i+1} \dots p_k^{\delta_k}$  où  $\delta_1 + \dots + (\delta_i+1) + \dots + \delta_k \leq (\alpha_1 + \dots + \alpha_k) - 1$

Alors  $d' \nmid n$  et  $d \mid d'$ , avec  $d' \neq d$  et  $d' \neq n$ .

$\Downarrow$   
 $G$  non maximal.

cqfd

### 3<sup>e</sup> méthode

#### préliminaire

Pro  $G \subset \Gamma$  groupe pas forcément commutatif  
 Alors  $G$  sous-groupe maximal  $\Leftrightarrow \Gamma/G$  simple

(Def : ~~H~~  $G$  est simple ssi  $G$  n'admet pas d'autres sous-groupes que  $\{e\}$  ou  $G$ )

Preuve: Par contraposée.

( $\Leftarrow$ ) Supposons  $G$  non maximal. Alors:  $\exists H / G \subsetneq H \subsetneq \Gamma$

Soit  $\chi$  la surjection canonique  $\chi: \Gamma \rightarrow \Gamma/G$ .  $\chi(H)$  = sous-groupe de  $\Gamma/G$ .

Alors  $\chi(H) \neq \{e\}$  sinon...

$\chi(H) \neq \Gamma/G$  sinon  $\forall x \in \Gamma \exists y \in H / \chi(y) = \chi(x)$

$\chi(yx^{-1}) = e$

Mais alors  $\exists \Gamma \subset G$ , absurde!

( $\Rightarrow$ ) Si  $\Gamma/G$  non simple,  $\exists H$  sous-groupe tel que  $\{0\} \subsetneq H \subsetneq \Gamma/G$

Alors  $G \subset \underbrace{\chi^{-1}(H)}_{\text{sous-groupe de } \Gamma} \subset \Gamma$

sous-groupe de  $\Gamma$   
 $\parallel \{0\}$

$\hookrightarrow$  car  $\chi$  surjective  
 $\subset$  toujours

\*  $\chi^{-1}(H) \neq G$ , sinon  $\chi(G) = \chi(\chi^{-1}(H)) = H$  absurde

\*  $\chi^{-1}(H) \neq \Gamma$ , " $\chi(\Gamma) = H$  absurde.  
 $\parallel$   
 $\Gamma/G$

d'où  $G$  non maximal. CQFD

Pro |  $H$  simple  $\Leftrightarrow H \simeq \mathbb{Z}/p\mathbb{Z}$  où  $p$  premier

( $\Rightarrow$ ) Si  $H$  est simple, soit  $x \in H$   $x \neq e$ . Alors  $\langle x \rangle = H \Leftrightarrow H \simeq \mathbb{Z}/p\mathbb{Z}$   
 et  $p$  premier (sinon  $H$  non simple)

( $\Leftarrow$ ) Évident.

exercice (suite)

Soit  $G \subset \mathbb{Z}/n\mathbb{Z}$ .  $G$  maximal  $\Leftrightarrow (\mathbb{Z}/n\mathbb{Z})/G$  simple

$$\Leftrightarrow [\mathbb{Z}/n\mathbb{Z} : G] \text{ premier}$$

$$\Leftrightarrow \frac{n}{\text{Card } G} \text{ premier}$$

$G$  maximal  $\Leftrightarrow \#G = d$  et  $\frac{n}{d}$  premier

## Révisions

1°  $A_n$  est engendré par les 3-cycles

2°  $A_n$  est simple  $n \geq 5$

3°  $\mathcal{I}_n$  est engendré par  $\underbrace{(1, 2, \dots, n-1)}_c$  et  $\underbrace{(n-1, n)}_t$

On a  $c^k t c^{-k} = (k, n)$  (le faire)

Ainsi  $\langle t, c \rangle \supset \{(n, n) \mid n \leq n-1\}$

On a :  $(n, n)(n, n)(n, n) = (n, n)$

et donc  $\langle t, c \rangle$  contient toutes les transpositions

## Valuation :

$$v_p(n!) = \sum_{k=1}^{\infty} E\left(\frac{n}{p^k}\right) \quad (p \in \mathcal{P}) \quad (\text{en fait somme finie})$$

$\mathbb{Z}$

$$n = \sum_{i=0}^{\infty} a_i p^i \quad 0 \leq a_i < p$$

(comme finie) Retrouvons la forme du cours :

$$\frac{n}{p^k} = \sum_{i=0}^{\infty} a_i p^{i-k} = \underbrace{\sum_{0 \leq i < k} a_i p^{i-k}}_A + \sum_{\substack{i \geq k \\ \xrightarrow{k \rightarrow i}}} a_i p^{i-k}$$

$$A = \frac{a_0}{p^k} + \dots + \frac{a_{k-1}}{p}$$

car  $a_i \leq p-1$

$$\leq (p-1) \left( \frac{1}{p^k} + \dots + \frac{1}{p} \right)$$

$$\leq \frac{p-1}{p} \frac{\frac{1}{p^k} - 1}{\frac{1}{p} - 1} = 1 - \frac{1}{p^k} < 1$$

$$\text{donc } E\left(\frac{n}{p^k}\right) = \sum_{i=k}^{\infty} a_i p^{i-k} \quad (\text{q } E(a+E) = E(a) \text{ ou } a \in \mathbb{C})$$

D'où :

$$\begin{aligned}
 v_p(n!) &= \sum_{k=0}^{\infty} \sum_{i \geq k} a_i p^{i-k} & \text{parce que } j=k \text{ et } i=k \\
 & & k=i-j \\
 &= \sum_{k=0}^{\infty} \sum_{j=0}^{\infty} a_{k+j} p^j = \sum_{j=0}^{\infty} p^j \left( \sum_{k=0}^{\infty} a_{k+j} \right) \\
 &= \sum_{i=0}^{\infty} a_i \sum_{j=0}^i p^j = \sum_{i=0}^{\infty} a_i \frac{p^{i+1} - 1}{p - 1}
 \end{aligned}$$

Pb : Nombre de zéros en base 10 de 100! ?

$$= \max \{ n \mid 10^n \mid 100! \}$$

$$10^n \mid 100! \Leftrightarrow 2^n \text{ et } 5^n \text{ divisent } 100! \Leftrightarrow \begin{cases} v_2(100!) \geq n \\ v_5(100!) \geq n \end{cases}$$

$$\Leftrightarrow n = \min(v_2(100!), v_5(100!))$$

$$\begin{aligned}
 \text{Calculons : } v_2(100!) &= E\left(\frac{100}{2}\right) + E\left(\frac{100}{4}\right) + E\left(\frac{100}{8}\right) + E\left(\frac{100}{16}\right) \\
 &\quad + E\left(\frac{100}{32}\right) + E\left(\frac{100}{64}\right)
 \end{aligned}$$

$$v_2(100!) = 50 + 25 + 12 + 6 + 3 + 1 = 97$$

$$\text{car } E\left(\frac{x}{2}\right) = E\left(\frac{E(x)}{2}\right)$$

$$v_5(100!) = 24$$

Nombre de zéros en base 12 de 100!

$$12^n \mid 100! \Leftrightarrow 2^{2n} \mid 100! \text{ et } 3^n \mid 100!$$

$$\Leftrightarrow \begin{cases} v_2(100!) \geq 2n \\ v_3(100!) \geq n \end{cases} \Leftrightarrow n = \min\left(\left\lfloor \frac{v_2(100!)}{2} \right\rfloor, v_3(100!)\right)$$

$$n = \min(48, 48) = 48$$

$$v_p(n!) = \sum_{k=1}^{\infty} E\left(\frac{n}{p^k}\right) = \frac{n - \alpha_p(n)}{p-1} \quad (\text{I})$$

$$E\left(\frac{E(n)}{m}\right) = E\left(\frac{n}{m}\right)$$

~~Calcul~~

Montrez que  $\frac{(2a)!(2b)!}{a!b!(a+b)!} \in \mathbb{N}$ . (2)

en utilisant la formule (I):  $v_p\left(\frac{C_{2a}^a C_{2b}^b}{C_{a+b}^a}\right) = \frac{1}{p-1} \left[ \underbrace{\alpha_p(a+b) + \alpha_p(a) + \alpha_p(b) - \alpha_p(2a) - \alpha_p(2b)}_{\text{montrer que c'est } \geq 0} \right]$

$$\begin{cases} a = \sum a_i p^i \\ b = \sum b_i p^i \end{cases} \quad \text{en base } p \quad \begin{cases} 2a = \sum (2a_i) p^i \\ 2b = \sum (2b_i) p^i \end{cases} \quad a+b = \sum (a_i + b_i) p^i$$

pas forcément en base  $p$ !

Il convient de faire très attention.

Contraintes:  $\forall i, a_i < \frac{p}{2}$  (aucune retenue pour  $2a, 2b, a+b$ )  
 $b_i < \frac{p}{2}$

Alors  $\alpha_p(a+b) = \alpha_p(a) + \alpha_p(b)$   
 $\alpha_p(2a) = 2\alpha_p(a)$   
 $\alpha_p(2b) = 2\alpha_p(b)$  et nous avons l'égalité.

Sinon: on l'admettra. Pour donner une démonstration correcte de (2), on utilisera plutôt la formule  $v_p(n!) = \sum_{k=1}^{\infty} E\left(\frac{n}{p^k}\right)$

$$v_p(n!) = \sum_{k=1}^{\infty} E\left(\frac{2a}{p^k}\right) + E\left(\frac{2b}{p^k}\right) - E\left(\frac{a}{p^k}\right) - E\left(\frac{b}{p^k}\right) - E\left(\frac{a+b}{p^k}\right) \geq 0$$

car:  $\forall \alpha, \beta \in \mathbb{R} \quad [2\alpha] + [2\beta] - [\alpha] - [\beta] - [\alpha + \beta] \geq 0$



(7)

Aut K ?

$$K = \{e, a, b, c\}$$

$$f \in \text{Aut } K \Rightarrow f|_{\{a,b,c\}} \in \mathcal{S}_{\{a,b,c\}}$$

$$\text{Aut } K \xrightarrow{\Phi} \mathcal{S}_{\{a,b,c\}}$$

$\Phi$  est injective (car si  $f$  et  $g$  coïncident sur  $\{a,b,c\}$ , elles coïncident <sup>sur</sup> en  $\{a,b,c\}$ .)

$\Phi$  est surjective : soit  $\sigma \in \mathcal{S}_{\{a,b,c\}}$ , alors  ~~$\exists f \in \text{Aut } K$~~  /

$$\exists f: K \rightarrow K \text{ par } f(e) = 1 \text{ et } f(x) = \sigma(x) \text{ pour } x \in \{a,b,c\}$$

$f$  est bijective. Reste à voir que c'est un morphisme.

$$f(xy) = f(x)f(y) ?$$

$$\text{Si } x=y, \text{ c'est vrai } f(x^2) = 1 = (f(x))^2$$

$$\text{Si } x=e, \quad " \quad f(x) = f(x) \text{ oui}$$

$$\text{Si } x \neq y \neq e \quad \left\{ \begin{array}{l} xy = z \quad \text{ou} \quad \{x, y, z\} = \{a, b, c\} \\ f(x)f(y) = f(xy) \text{ car } \{f(x), f(y), f(x)f(y)\} \\ \text{d'où} \quad \quad \quad = \{a, b, c\} \end{array} \right.$$

$$\begin{array}{ccc} \cancel{f(xy)} & \{x, y, xy\} & \\ \downarrow & \searrow & \swarrow \\ & \{\sigma(x), \sigma(y), \sigma(x)\sigma(y)\} & \end{array}$$

Rappel :  $K$  = corps commutatif (ce ne sera pas  $\mathbb{R}$ !)

$E = K$ -espace vectoriel

$$f: E \rightarrow E \text{ affine} \Leftrightarrow \exists a \in E \quad \exists l \in \text{End}(E) / f = t_a \circ l$$

$$\forall x \in E \quad f(x) = a + l(x)$$

$$GA(E) = \{\text{applications affines bijectives}\}$$

$$GA(E) \xrightarrow{\Phi} E \times GL(E)$$

$\Phi$  est bijective

$$t_a \circ l \xrightarrow{\quad} (a, l)$$

car 
$$E \times GL(E) \xrightarrow{\Phi} GA(E)$$
  

$$(a, l) \mapsto t_a \circ l$$

et 
$$GA(E) \xrightarrow{\Psi} E \times GL(E)$$
  

$$g \mapsto (g(0), t_{-g(0)} \circ g)$$

Ainsi 
$$GA(E) \xrightarrow[\cong]{\Psi \circ \Phi} E \times GL(E)$$

On transporte les structures grâce à  $\Phi$ , sur  $E \times GL(E)$  :

$$(a, l) * (a', l') = (t_a \circ l) \circ (t_{a'} \circ l')$$

$$= t_{a+l(a')} \circ (l \circ l')$$

Ainsi : 
$$(a, l) * (a', l') = (a + l(a'), l \circ l')$$

$\neq \underbrace{(a+a', l \circ l')}_{\text{loi habituelle}}$

On définit sur :

$K \times \text{Aut } K$

une loi "bizarre" grâce aux rappels concernant les espaces affines.

On définit la loi sur  $K \times \text{Aut } K$  par :

$$(x, \sigma)(x', \sigma') = (x \sigma'(x'), \sigma \circ \sigma')$$

Prendons  $K = \mathbb{Z}/2\mathbb{Z}$

$E = K$  (de dimension 2 sur  $K$ )  
 $K = (\mathbb{Z}/2\mathbb{Z})^2$

$$GA(K) = \underbrace{\mathcal{P}(K)}_{\text{permutations de } K}$$

- $GA(K) \subset \mathcal{P}(K)$  évident
- Inversement



$K = \{0, a, b, c\}$  Soit  $\sigma \in \mathcal{P}(K)$

$(a, b, c)$  est un repère affine de  $K$  puisque :  $\{x, y, z\}$  distincts deux à deux, dans  $K$   
 (alors ils sont non colinéaires)

Regardons  $\sigma(a)$   $\sigma(b)$   $\sigma(c)$

donc  $\sigma(a)$ ,  $\sigma(b)$  et  $\sigma(c)$  sont distincts 2 à 2

$$\exists! f \in GA(K) \text{ telle que } \begin{cases} f(a) = \sigma(a) \\ f(b) = \sigma(b) \\ f(c) = \sigma(c) \end{cases} \Rightarrow \text{f et } \sigma \text{ coïncident sur } K$$

Donc

$$GA(K) = J(K)$$

Que dire de  $GL(K)$ ?  $GL(K)$  est l'ensemble des applications affines de  $K$  qui laissent 0 invariant. Or  $GA(K) = J(K) \Rightarrow GL(K)$  isomorphe à  $J_{\{a,b,c\}}$  (on a fixé 0), ~~donc~~ c.à.d isomorphe à  $\text{Aut } K$

$$\text{d'où } J_4 \simeq K \times J_3$$

$$\underbrace{GA(K)}_{\substack{J(K) \\ \uparrow \\ J_4}} \simeq K \times \underbrace{GL(K)}_{\substack{\text{on a vu que c'est isomorphe à } J_{\{a,b,c\}} = J_3 \\ \text{produit bijectif!}}}$$

d'où

$$J_4 \simeq K \times J_3$$

↑  
produit bijectif.

(14)

$a$  est un carré  $\Leftrightarrow a = p_1^{2\alpha_1} \dots p_k^{2\alpha_k}$   $p_1, \dots, p_k =$  nombres premiers.

Montrons que  $a$  est un carré  $\Leftrightarrow$  le nombre de diviseurs de  $a$  est impair

( $\Rightarrow$ )  $a$  possède  $(2\alpha_1+1) \dots (2\alpha_k+1) =$  un nombre impair de diviseurs.

( $\Leftarrow$ ) Soit  $a = p_1^{\beta_1} \dots p_k^{\beta_k}$  et  $(\beta_1+1) \dots (\beta_k+1)$  impair  $\Rightarrow \beta_i+1$  impair  $\Rightarrow \beta_i$  pair.

CQFD

(10)

Lemme:  $\forall a, b \in \mathbb{Z} \quad \forall p \in \mathcal{P} \quad v_p(a+b) \geq \min(v_p(a), v_p(b))$  (L)

En effet:  $\begin{cases} a = p^\alpha a' & \Delta(a', p) = 1 \\ b = p^\beta b' & \Delta(b', p) = 1 \end{cases} \Rightarrow a+b = p^\alpha (a' + p^{\beta-\alpha} b')$  si  $\alpha \leq \beta$   
donc  $v_p(a+b) \geq \min(v_p(a), v_p(b))$

Soit  $a_i \in \mathbb{Z}$ ,  $\sum_{i=1}^n a_i = 0$ .  $\forall p \in \mathcal{P}$ ,  $\min\{v_p(a_i) / 1 \leq i \leq n\}$  est atteint au moins 2 fois.

Supposons que  $\min_{i \in \{1, n\}} (v_p(a_i)) = v_p(a_1)$ .

Or  $\sum_{i=2}^n a_i = -a_1$  (1)

et  $v_p\left(\sum_{i=2}^n a_i\right) \geq \min_{i \in \{2, n\}} (v_p(a_i))$ . (voir lemme) (2)

Si  $\min_{i \in \{2, n\}} (v_p(a_i)) \neq v_p(a_1)$ , alors  $v_p\left(\sum_{i=2}^n a_i\right) > v_p(a_1)$  ce qui est absurde en égard à (1).

Le minimum des valuations  $p$ -adiques est atteint au moins 2 fois.

CQFD } on conclut par l'absurde  
un raisonnement direct

Généralisation de cette propriété

(1) et (2)  $\Rightarrow v_p(a_1) \geq \min_{i \in \{2, n\}} (v_p(a_i))$

On sait définir la valuation  $p$ -adique d'un nombre rationnel :

$$\forall m = \frac{p_0}{q_0} \in \mathbb{Q} \quad v_p(m) = v_p(p_0) - v_p(q_0)$$

$\Downarrow$   
 $\exists k \in \{2, n\} / v_p(a_1) = v_p(a_k)$

En faisant la même démonstration que ci-dessus, on constate que, si  $\sum_{i=1}^n a_i = 0$

où  $a_i \in \mathbb{Q}$ , alors  $\min_{i \in [1, n]} (v_p(a_i))$  est atteint au moins 2 fois.

Notons (P) cette propriété.

Montrer que  $S_n = 1 + \dots + \frac{1}{n}$  ( $n \geq 2$ ) n'est jamais entier

~~Supposons, par l'absurde, que  $S_n \in \mathbb{N} \subset \mathbb{Q}$ . Alors :~~

•  $S_n \in \mathbb{Q} \quad 1 + \dots + \frac{1}{n} - S_n = 0$

2) d'après la propriété (P) :  $\min_{x \in [1, n]} (v_2(\frac{1}{x}), v_2(S_n))$  est atteint au moins 2 fois.

• Si nous montrons que  $\min_{x \in [1, n]} (v_2(\frac{1}{x}))$  est atteint seulement en une valeur de  $x$ , et que cette valeur est négative, alors on aura montré que  $v_2(S_n) = \min_{x \in [1, n]} (v_2(\frac{1}{x})) < 0$

c.à.d :  $S_n \notin \mathbb{N}$ .

Preuve :

• Comme  $v_2(\frac{1}{2}) = -1$ ,  $\min_{x \in [1, n]} (v_2(\frac{1}{x})) < 0$

Comme  $v_2(\frac{1}{x}) = -v_2(x)$ , il suffit de montrer que  $v_2(x)$  atteint une fois son maximum pour  $x = 1, \dots, n$ . Pour cela, on observera que :

$$v_2(1) = 0$$

$$v_2(2) = 1$$

$$v_2(3) = 0$$

$$v_2(4) = 2 \leftarrow 4 = 2^2$$

$$v_2(5) = 0 \quad \text{maximum unique.}$$

$$v_2(6) = 1$$

NB : Ça ne marche pas pour  $p \in \mathcal{P}$   
 $p \geq 2$

car, au lieu d'être atteint seulement en  $2^x$ , il le sera <sup>peut-être</sup> en tous les nombres de la forme  $p^x, 2p^x, \dots, (p-1)p^x$

$$\forall n \in \mathbb{N} (n \geq 2) \quad \exists \alpha \in \mathbb{N} / 2^\alpha \leq n < 2^{\alpha+1}$$

Alors  $\boxed{\forall x \in [1, n] \atop x \neq 2^\alpha \Rightarrow v_2(x) < \underbrace{v_2(2^\alpha)}_{= \alpha}}$

En effet : par l'absurde. Si  $v_2(x) = \alpha' \geq \alpha$ , alors  $x = 2^{\alpha'} q$   $\alpha' \geq \alpha$  et  $\Delta(q, 2) = 1$   
↑  
en fait, la contradiction.

Si  $q=1$   $n=2^{\alpha'}$ . Mais alors  $\alpha' \geq \alpha$  et  $n \neq 2^{\alpha} \Rightarrow n \notin [1, n]$ , absurde.  
 Si  $q \neq 1$ ,  $q \geq 2 \Rightarrow n = 2^{\alpha'} q > 2^{\alpha+1} \Rightarrow n \notin [1, n]$  absurde.

CQFD

(14)  $a \in \mathbb{N}$

$$\mathcal{D}(a) = \{d / d \text{ divise } a\}$$

$$\# \mathcal{D}(a) \text{ impair} \Leftrightarrow \exists b \in \mathbb{N} / a = b^2$$

$$\mathcal{D} = \mathcal{D}' \cup \mathcal{D}''$$

$$\begin{cases} \mathcal{D}' = \{d / d \leq \frac{a}{d}\} \\ \mathcal{D}'' = \{d / d \geq \frac{a}{d}\} \end{cases} \quad (\text{et } d|a, \text{ évidemment})$$

On remarque que :  $f: \mathcal{D}' \rightarrow \mathcal{D}''$  bijective. ( $f$  involutive)  
 $d \mapsto \frac{a}{d}$

$$\text{donc } \# \mathcal{D}' = \# \mathcal{D}'' = n$$

$$\# \mathcal{D} = 2n - \# (\mathcal{D}' \cap \mathcal{D}'')$$

"  
 $\emptyset$  ou contient un seul élément  $d / d^2 = a$ .

D'où

$$\begin{cases} \# \mathcal{D} \text{ pair} \\ \# (\mathcal{D}' \cap \mathcal{D}'') = 0 \Leftrightarrow a \neq \text{carré} \Leftrightarrow \# \mathcal{D} \text{ pair} \\ \# (\mathcal{D}' \cap \mathcal{D}'') = 1 \Leftrightarrow a = \text{carré} \Leftrightarrow \# \mathcal{D} \text{ impair} \end{cases}$$

⑧  $\text{Aut}(\mathbb{Z}/n\mathbb{Z})$  ?

On considère  $\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \longrightarrow \mathbb{Z}/n\mathbb{Z}$

$$f \longmapsto f(1) = a \quad (1)$$

Si  $f \in \text{Aut}(\mathbb{Z}/n\mathbb{Z})$ ,  $f(1)$  = élément d'ordre  $n$  (car  $f$  conserve l'ordre.)

Il y a  $\varphi(n)$  él. d'ordre  $n$  dans  $\mathbb{Z}/n\mathbb{Z}$

$$f(1) = a \quad a \in \mathbb{Z} \text{ et } \Delta(a, n) = 1$$

Inversement, si  $f(1) = a$   $\Delta(a, n) = 1$ , alors  $f$ , automorphisme, est parfaitement déterminé.

$$\# \text{Aut}(\mathbb{Z}/n\mathbb{Z}) = \varphi(n)$$

Et la structure de groupe de  $(\text{Aut}(\mathbb{Z}/n\mathbb{Z}), \circ)$  ?

$$f \circ g(1) = f(g(1)) = f(b \cdot 1) = b f(1) = ba = \widehat{ba}$$

donc  $(\text{Aut}(\mathbb{Z}/n\mathbb{Z}), \circ)$  est commutatif, ce qui ne sautait pas aux yeux

$$\text{De plus : } f \circ g(1) = \widehat{ba} = \widehat{b} \widehat{a} = \widehat{f(1)} \times \widehat{g(1)} \quad (2)$$

Remarque:  $A$  anneau  $U(A) = \{x \in A / \exists x' \quad xx' = 1\}$

$U(A)$  est un groupe pour  $\times$

un exemple  $U(\mathbb{Z}) = \{-1, 1\}$

$$U(K) = K^* \quad (\text{si } K = \text{corps})$$

On a donc montré en (1) et (2), que  $\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq U(\mathbb{Z}/n\mathbb{Z})$

$$\textcircled{9} \quad N(a, b) = \frac{(2a)!(2b)!}{a!b!(a+b)!}$$

On sait que

$$\boxed{\varphi_p(x!) = \sum_{k=1}^{\infty} E\left(\frac{x}{p^k}\right)}$$

Preuve de la formule :

Si  $x < p$ , la formule est vraie.

Si  $x \geq p$ , on écrit:  $x! = \underbrace{1.2.3.\dots}_{\substack{\uparrow \\ \text{pas de facteur } p \\ \text{dans la d.n.p.}}} p \dots \underbrace{2.p.\dots}_{\substack{\uparrow \\ \text{pas de facteur } p \\ \text{(d.n.p.)}}} a.p.\dots x$

~~$(a+1)p$~~

$$v_p(x!) = v_p(p^a a!)$$

$$\text{et } a = E\left(\frac{x}{p}\right)$$

$$\text{Donc } v_p(x!) = E\left(\frac{x}{p}\right) + v_p\left(E\left(\frac{x}{p}\right)!\right)$$

Et, on recommence :

$$v_p(x!) = E\left(\frac{x}{p}\right) + E\left(\frac{E\left(\frac{x}{p}\right)}{p}\right) + v_p\left(E\left(\frac{E\left(\frac{x}{p}\right)}{p}\right)!\right) \quad (1)$$

Lemme :  $\left\lfloor \frac{\lfloor y \rfloor}{p} \right\rfloor = \left\lfloor \frac{y}{p} \right\rfloor$

$$y = \lfloor y \rfloor + a \quad a < 1$$

$$\lfloor y \rfloor = pq + r \quad r \leq p-1$$

$$\frac{\lfloor y \rfloor}{p} = q + \frac{r}{p} \quad \left\lfloor \frac{\lfloor y \rfloor}{p} \right\rfloor = q$$

$$\frac{y}{p} = \frac{\lfloor y \rfloor + a}{p} = q + \frac{r+a}{p} \quad \text{et } r+a < p \Rightarrow \frac{r+a}{p} < 1$$

$$\text{donc } \left\lfloor \frac{y}{p} \right\rfloor = q \quad \text{CQFD}$$

$$(1) \text{ donne } v_p(x!) = \left\lfloor \frac{x}{p} \right\rfloor + \left\lfloor \frac{x}{p^2} \right\rfloor + \dots + \left\lfloor \frac{x}{p^k} \right\rfloor$$

Retour à l'exercice :

$$v_p(N(a,b)) = v_p(2a!) + v_p(2b!) - v_p(a!) - v_p(b!) - v_p((a+b)!)$$

$$= \sum_{k=1}^{\infty} \left[ \left\lfloor \frac{2a}{p^k} \right\rfloor + \left\lfloor \frac{2b}{p^k} \right\rfloor - \left\lfloor \frac{a}{p^k} \right\rfloor - \left\lfloor \frac{b}{p^k} \right\rfloor - \left\lfloor \frac{a+b}{p^k} \right\rfloor \right]$$



• Montrons que :

$$\forall x, y \in \mathbb{R} \quad [2x] + [2y] - [x] - [y] - [x+y] \geq 0$$

Preuve :

$$\text{Envisager les cas } \left\{ \begin{array}{l} x = [x] + a \quad a < 1 \\ y = [y] + b \quad b < 1 \end{array} \right.$$

$$\textcircled{1} \quad a < \frac{1}{2} \text{ et } b < \frac{1}{2}$$

$$\textcircled{2} \quad a < \frac{1}{2} \text{ et } b \geq \frac{1}{2}$$

$$\textcircled{3} \quad a \geq \frac{1}{2} \text{ et } b \geq \frac{1}{2}$$

On calcule l'expression dans chacun de ces cas. On trouve chaque fois 1 ou 0.

2-méthode

$$N(a+1, b) + N(a, b+1) = 4 N(a, b)$$

$$\text{Par récurrence} \quad N(a, b+1) = \underbrace{4 N(a, b)}_{\in \mathbb{N}} - \underbrace{N(a+1, b)}_{\in \mathbb{N}}$$

$\textcircled{13}$  Prendre  $H = \mathbb{Z}$

$$H' = n\mathbb{Z} \quad (n \neq 1, n \neq 0)$$

$$\text{et } \mathbb{Z} \longrightarrow n\mathbb{Z}$$

$x \mapsto nx$  est un isomorphisme de groupes.

$$\text{et pourtant } \mathbb{Z}/n\mathbb{Z} \not\cong \mathbb{Z}/\mathbb{Z}$$

$$\quad \quad \quad \underbrace{\quad}_{\{0\}}$$

UNIVERSITÉ DE NICE  
INSTITUT DE MATHÉMATIQUES  
ET SCIENCES PHYSIQUES

PARC VALROSE  
06034 NICE CEDEX  
TÉL. (93) 51.91.00

MATHÉMATIQUES

M1 Algèbre et Arithmétique.

Feuille N°4.

x 1° Montrer que pour qu'un produit de groupes soit cyclique, il faut et il suffit qu'ils le soient tous deux, et que leurs cardinaux soient premiers entre eux.

x 2° Résoudre les systèmes de congruences :

$$\begin{cases} x \equiv 3 & (4) \\ x \equiv 0 & (3) \end{cases}$$

$$\begin{cases} x \equiv 2 & (6) \\ x \equiv 5 & (9) \end{cases} \quad \begin{cases} x \equiv 15 & (32) \\ x \equiv 7 & (26) \end{cases} \quad (\text{fait au tableau.})$$

x 3° (Pb du cuisinier chinois) Une bande de 17 pirates s'est emparée d'un butin composé de pièces d'or d'égale valeur. Ils décident qu'une fois arrivés à terre ils partageront également les pièces d'or entre eux, et donneront le reste, soit trois pièces d'or au cuisinier chinois. Mais les pirates se querellent et six d'entre eux sont tués. Le cuisinier recevrait alors 4 pièces.

Dans un naufrage ultérieur, seul le butin, 6 pirates et le cuisinier sont sauvés et le partage laisserait 5 pièces d'or à ce dernier. Quelle est alors la fortune minimale que peut espérer le cuisinier quand il décide d'empoisonner le reste des pirates ?

9.01.78

4.7 Soit  $H$  un sous-groupe de  $(\mathbb{Z}^2, +)$  qu'on suppose non réduit à  $\{(0,0)\}$ .

A) On suppose que pour tout couple  $((a,b), (c,d))$  d'éléments de  $H$  on a  $ad - bc = 0$ .

$\alpha)$  S'il existe un élément  $(0,b) \neq 0$  dans  $H$ , alors tout élément de  $H$  est de cette forme et  $H$  est engendré par un élément; même résultat pour  $(a,0) \neq 0$  dans  $H$ .

$\beta)$  Sinon, soit  $(a,b) \in H$ , avec  $d = \text{pgcd}(a,b)$  et  $d = \min \{ \text{pgcd}(x,y) \mid (x,y) \in H, x \neq 0, y \neq 0 \}$  (on prend les  $\text{pgcd} > 0$ )

alors,  $(a,b)$  engendre  $H$ .

B) On suppose maintenant qu'il existe des couples  $((a,b), (c,d))$  dans  $H \times H$  vérifiant  $ad - bc \neq 0$ , et soit un tel couple vérifiant en outre  $\delta = ad - bc = \inf \{ vx - uy \mid \begin{matrix} (x,y) \in H \\ (u,v) \in H, vx - uy > 0 \end{matrix} \}$

$\alpha)$  On considère les applications  $\varphi$  et  $\psi$  de  $H$  dans  $\mathbb{Z}$  définies par  $\varphi(x,y) = ay - bx$  et  $\psi(x,y) = cy - dx$ . Montrer que  $\varphi(H)$  et  $\psi(H)$  sont des sous-groupes de  $\mathbb{Z}$ .

$\beta)$  En déduire  $\varphi(H) = \psi(H) = \delta\mathbb{Z}$ .

$\gamma)$  Montrer que  $\{(a,b), (c,d)\}$  engendre  $H$ .

[Si  $(x,y) \in H$ ,  $\delta \mid \varphi(x,y)$  et  $\delta \mid \psi(x,y)$ ].

1<sup>re</sup> méthode : Démonstration :

$$① \quad G_1 \times G_2 \text{ cyclique} \Leftrightarrow G_1 \text{ et } G_2 \text{ cycliques et } \Delta(n_1, n_2) = 1$$

$$(\Leftrightarrow) \boxed{G \text{ cyclique} \Leftrightarrow \forall d \mid n \quad \# \{x \in G / dx = 0\} \leq d} \quad (\text{rappel de cours})$$

$$d \mid d_1 n_1 \quad \text{et } n = n_1 n_2$$

$$\text{On va essayer d'écrire : } d = d_1 d_2 \text{ où } d_1 \mid n_1 \text{ et } d_2 \mid n_2.$$

(Ce n'est pas toujours le cas :  $n_1=4, n_2=6$ )

$$\text{Soit } d \mid n_1 n_2 \quad d_1 = \text{pgcd}(d, n_1) \Rightarrow \begin{cases} d = d_1 d_2 \\ n_1 = d_1 n'_1 \end{cases} \text{ et } \Delta(d_2, n'_1) = 1$$

$$d_1 d_2 \mid n_1 n_2 \Rightarrow d_2 \mid n_2 n'_1 \Rightarrow d_2 \mid n_2 \text{ d'où } n_2 = d_2 n'_2 \quad (\text{gauche})$$

$$\text{donc } d = d_1 d_2 \text{ où } d_1 \mid n_1 \text{ et } d_2 \mid n_2$$

Montrons que cette décomposition  $d = d_1 d_2$  est unique, si  $\Delta(n_1, n_2) = 1$  :

$$\text{Si } \Delta(n_1, n_2) = 1 \quad d_1 d_2 = d'_1 d'_2 = d \text{ divise } n \Rightarrow d_1 = d'_1, d_2 = d'_2$$

$$\text{En effet } \left. \begin{array}{l} d_1 \mid d'_1 d'_2 \\ \text{et} \\ \Delta(d_1, d'_2) = 1 \end{array} \right\} \Rightarrow d_1 \mid d'_1 \text{ de même } d'_1 \mid d_1 \Rightarrow d_1 = d'_1$$

Conclusion :

Retour à l'exercice :

$$d_1 \mid n_1, \quad \# \overbrace{\{x_1 \in G_1 / d_1 x_1 = 0\}}^{E_1} \leq d_1$$

$$d_2 \mid n_2, \quad \# \underbrace{\{x_2 \in G_2 / d_2 x_2 = 0\}}_{\overline{E_2}} \leq d_2$$

On cherche l'ensemble des couples  $(x_1, x_2)$  tels que  $d(x_1, x_2) = 0$ .

$$d(x_1, x_2) = 0 \Leftrightarrow \begin{cases} d_1 d_2 x_1 = 0 \\ d_1 d_2 x_2 = 0 \end{cases} \Leftrightarrow (*) \begin{cases} d_1 x_1 = 0 \\ d_2 x_2 = 0 \end{cases}$$

(\*)  
En effet:

$$d_1 x_1 \in G_1 \quad d_2(d_1 x_1) = 0 \Leftrightarrow \underbrace{\omega(d_1 x_1)} \mid d_2$$

c'est un diviseur de  $n_1$   
et aussi diviseur de  $n_2$  car  $d_2 \mid n_2 \Rightarrow \omega(d_1 x_1) = 1$   
Donc  $d_1 x_1 = 0$

$$\text{Donc } E = \{(x_1, x_2) / d(x_1, x_2) = 0\} = E_1 \times E_2$$

$\Downarrow$

$$\text{Card } E \leq d_1 \times d_2 = d$$

( $\Rightarrow$ ) Inversement, supposons que  $\text{Card } E \leq d$ .

$$\bullet d_1 \mid n_1, \# \underbrace{\{x_1 \in G_1 / d_1 x_1 = 0\}}_{E_1} \leq d_1$$

$$d_1 \mid n_1 \Rightarrow d_1 \mid n \quad \text{et} \quad \# \{x \in G / d_1 x = 0\} \leq d_1$$

$$x_1 \in E_1 \hookrightarrow (x_1, 0) \in E$$

$$\text{donc } \text{Card } E_1 \leq \text{Card } E \leq d_1$$

$$\bullet \text{ Soit } d = \gcd(n_1, n_2) \text{ un diviseur commun } \tilde{a} \ n_1 \text{ et } \tilde{a} \ n_2$$

$$d \mid n_1 \text{ et } d \mid n_2 \Rightarrow d \mid n$$

$$\text{On sait que } \# \{x \in G / dx = 0\} = d$$

$$\text{Or } \{x \in G / dx = 0\} = \{x_1 \in G_1 / d x_1 = 0\} \times \{x_2 \in G_2 / d x_2 = 0\}$$

$\Downarrow$

$$d^2 = d$$

$\Downarrow$

$$d = 1$$

2<sup>e</sup> méthode : à montrer :  $G = G_1 \times G_2$  cyclique  $\Leftrightarrow G_1$  et  $G_2$  cycliques et  $\Delta(n_1, n_2) = 1$

$$(\Leftarrow) \begin{array}{l} G_1 = \langle h \rangle \\ G_2 = \langle k \rangle \end{array} \quad \text{Alors } \omega(h, k) = \text{ppcm}(\omega(h), \omega(k)) = n_1 n_2 \Rightarrow (h, k) \text{ engendre } G, \\ \text{(cf. lemme)}$$

$$(\Rightarrow) \text{ Si } \omega(h, k) = \frac{n_1 n_2}{\Delta(n_1, n_2)} \\ \text{ppcm}(\omega(h), \omega(k))$$

Posons  $\begin{cases} n_1 = \omega(h) n'_1 \\ n_2 = \omega(k) n'_2 \end{cases}$ . Alors on obtient :  $\text{ppcm}(\omega(h), \omega(k)) = \omega(h) \omega(k) n'_1 n'_2$

$$1 = n'_1 n'_2 \Delta(\omega(h), \omega(k))$$

$\Leftrightarrow$

$$n'_1 = n'_2 = \Delta(\omega(h), \omega(k)) = 1$$

Donc  $\begin{cases} \omega(h) = n_1 \\ \omega(k) = n_2 \end{cases}$  et  $\Delta(n_1, n_2) = 1$ . CQFD

Lemme  $\omega(h, k) = \text{ppcm}(\omega(h), \omega(k))$

En effet  $n(h, k) = (0, 0) \Leftrightarrow \begin{cases} nh = 0 \Rightarrow \omega(h) | n \\ nk = 0 \Rightarrow \omega(k) | n \end{cases} \Rightarrow \text{ppcm}(\omega(h), \omega(k)) | n$

et  $\text{ppcm}(\omega(h), \omega(k)) (h, k) = (0, 0)$ , donc  $\omega(h, k) = \text{ppcm}(\omega(h), \omega(k))$ .  
(oui)

Remarque :

l'exercice contient le théorème chinois.

$$\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \text{ est cyclique, isomorphe à } \mathbb{Z}/ab\mathbb{Z}, \text{ si } \Delta(a, b) = 1$$

③ n pièces d'or

- a) 17 pirates  $n \equiv 3 \pmod{17}$   
 b) 11 pirates  $n \equiv 4 \pmod{11}$   
 c) 6 pirates  $n \equiv 5 \pmod{6}$

(1)  $\Delta(11, 17) = 1$  ~~divise 4-3~~  $\Rightarrow$  solution unique modulo  $\text{ppcm}(17, 11)$   
 $= 17 \times 11 = 187$

$$n = 3 + 17l$$

$$3 + 6l \equiv 4 \pmod{11}$$

$$6l \equiv 1 \pmod{11} \quad \text{et } 6 \cdot 2 = 1 \text{ dans } \mathbb{Z}/11\mathbb{Z}$$

$$\Downarrow$$

$$l \equiv 2 \pmod{11}$$

$$l = 2 + 11u \quad \text{d'où } n = 37 + 187u \quad u \in \mathbb{Z}$$

$$(2) \begin{cases} n \equiv 37 \pmod{187} \\ n \equiv 5 \pmod{6} \end{cases}$$

$\Delta(187, 6) \Rightarrow \exists!$  solution modulo  $187 \times 6 = 1122$

$$\text{On a} \quad 187l + 37 \equiv 5 \pmod{6}$$

$$187l \equiv 4 \pmod{6}$$

$$l \equiv 4 \pmod{6}$$

d'où  $n = 1122u + 785$ . Le plus petit gain possible est donc 785 pièces

Rappel : Suite exacte

$$0 \rightarrow \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \rightarrow \mathbb{Z}/d\mathbb{Z} \rightarrow 0$$

## Exercice (4)

● Soit  $H$  un sous-groupe de  $(\mathbb{Z}^2, +)$ ,  $H \neq \{(0,0)\}$

A) Si  $\forall (a,b), (c,d) \in H^2$  on a  $ad - bc = 0$

$\alpha)$  S'il existe un élément  $(0,b) \neq (0,0)$  dans  $H$ , alors tout élément de  $H$  est de cette forme et  $H$  est engendré par un élément  $(0,b)$ .

Même résultat pour  $(a,0) \in H$ .

$\beta)$  Sinon, soit  $(a,b) \in H$  avec  $d = \Delta(a,b) = \min \{ \Delta(x,y) \mid (x,y) \in H, x \neq 0, y \neq 0 \}$  (on prend le pgcd  $> 0$ ). Alors  $(a,b)$  engendre  $H$ .

● B) Si  $\exists ((a,b), (c,d)) \in H^2$  tels que  $ad - bc \neq 0$ . Soit un tel couple vérifiant, en outre  $\delta = ad - bc = \inf \{ vx - uy \mid \begin{matrix} (x,y) \in H \\ (u,v) \in H \text{ et } vx - uy > 0 \end{matrix} \}$

$\alpha)$  On considère les applications  $\varphi$  et  $\psi$  de  $H$  dans  $\mathbb{Z}$  définies par  $\varphi(x,y) = ay - bx$  et  $\psi(x,y) = cy - dx$ . Montrer que  $\varphi(H)$  et  $\psi(H)$  sont des sous-groupes de  $\mathbb{Z}$

$\beta)$  En déduire  $\varphi(H) = \psi(H) = \delta\mathbb{Z}$

$\gamma)$  Montrer que  $((a,b), (c,d))$  engendrent  $H$  et que  $H \simeq \mathbb{Z}^2$

[Indications : Si  $(x,y) \in H$   $\delta \mid \varphi(x,y)$  et  $\delta \mid \psi(x,y)$ ]

## Solution

A)  $\alpha)$   $\forall (a_1, a_2) \in H$   $a_1 b - a_2 0 = 0 \Rightarrow a_1 = 0$  oui

Soit  $\beta: \mathbb{Z} \rightarrow \mathbb{Z}^2$  est un isomorphisme  
 $b \mapsto (0, b)$

$H \subset \beta(\mathbb{Z})$   $\beta^{-1}(H) =$  sous-groupe de  $\mathbb{Z} = n\mathbb{Z}$  et  $\beta(\beta^{-1}(H)) = H$  car  $H \subset \text{Im } \beta$

d'où  $H = \beta(n\mathbb{Z}) \Rightarrow H$  engendré par  $\beta(n) = (0, n)$



$$\beta) (x, y), (a, b) \in H \Rightarrow xb - ay = 0 \Rightarrow xb = ya$$

$$\begin{aligned} d &= \Delta(a, b) \\ a &= da' \\ b &= db' \end{aligned} \quad \text{d'où} \quad xb' = ya' \quad (1)$$

$$a' \mid xb' \text{ et } \Delta(a', b') = 1 \Rightarrow a' \mid x \Rightarrow \exists n_1 \in \mathbb{Z} / x = n_1 a'$$

$$\text{D'après (1)} : y = n_1 b'$$

$$\text{Ainsi : } \begin{cases} x = n_1 a' \\ y = n_1 b' \end{cases} \quad (2)$$

Comme  $\delta = \Delta(x, y) = \Delta(n_1 a', n_1 b') = n_1 \geq d$ , on peut faire la division euclidienne de  $n_1$  par  $d$ :

$$n_1 = dq + r \quad \text{où} \quad 0 \leq r < d$$

$$\text{D'après } \begin{cases} x = dq a' + r a' = q a + r a' \\ y = dq b' + r b' = q b + r b' \end{cases} \Rightarrow \underbrace{(x, y)}_{\in H} = \underbrace{q(a, b)}_{\in H} + r(a', b')$$

donc  $r(a', b') \in H$ , mais  $\Delta(a', b') = 1 \Rightarrow \Delta(r a', r b') = r < d$  ! absurde.

Donc  $r = 0$ , autrement dit :  $n_1 = dq$ .

$$(2) \Rightarrow \begin{cases} x = q a \\ y = q b \end{cases}$$

On a montré que  $(x, y) \in H \Rightarrow \exists q \in \mathbb{Z} \quad (x, y) = q(a, b)$ , ce qui prouve que  $H = \langle (a, b) \rangle$ .

cq.c.d

B)  $\alpha) \varphi : H \rightarrow \mathbb{Z}$  sont des morphismes de groupe.

donc  $\varphi(H)$  et  $\psi(H)$  = sous-groupes de  $\mathbb{Z}$ .

$$\beta) \text{ Posons } \varphi(H) = l\mathbb{Z} \quad (l > 0)$$

$$\begin{aligned} \bullet \varphi(c, d) = ad - bc = \delta &\Rightarrow \delta\mathbb{Z} \subset l\mathbb{Z} \Rightarrow l \leq \delta \\ \bullet \exists (x, y) \in H / \varphi(x, y) = ay - bx = l > 0 &\Rightarrow \delta \leq ay - bx = l \Rightarrow \delta \leq l \end{aligned} \quad \left. \vphantom{\begin{aligned} \bullet \varphi(c, d) = ad - bc = \delta \\ \bullet \exists (x, y) \in H / \varphi(x, y) = ay - bx = l > 0 \end{aligned}} \right\} \delta = l$$

Ainsi

$$\boxed{\varphi(H) = \delta\mathbb{Z}}$$

(On remarque que tout marche bien parce que les bornes sont atteintes)

(mê chose avec  $\psi$ )

8) On doit montrer que

$$\forall (x, y) \in H \quad \exists n, m \quad / \quad (x, y) = n(a, b) + m(c, d)$$

$$(n, y) = (na + mc, nb + md)$$

$$\begin{cases} x = na + mc \\ y = nb + md \end{cases}$$

d'où :

$$\begin{cases} n = \frac{\begin{vmatrix} x & c \\ y & d \end{vmatrix}}{ad - bc} = \frac{dx - cy}{\delta} \in \mathbb{Z} \quad (\text{car } \delta \mid dx - cy) \\ m = \frac{\begin{vmatrix} a & x \\ b & y \end{vmatrix}}{ad - bc} = \frac{ay - bx}{\delta} \in \mathbb{Z} \quad (\text{car } \delta \mid ay - bx) \end{cases}$$

CGFD.

On a  $\Phi : \mathbb{Z}^2 \rightarrow H$

$$(n, m) \mapsto n(a, b) + m(c, d) \quad (\Phi \text{ est un isomorphisme de groupes})$$

(Remarque : interprétation géométrique,  $\det \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \text{aire du parallélogramme construit sur } \begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} c \\ d \end{pmatrix}$ )

### Exercice

- Soit  $G$  un groupe.  $D(G)$  = groupe dérivée  $\doteq$  plus petit sous-groupe de  $G$  contenant tous les éléments de la forme  $x y x^{-1} y^{-1}$  ( $x, y \in G$ ).

Montrer que, si  $u$  = endomorphisme de  $G$ , alors

1°  $u(D(G)) \subset D(G)$

2° si  $H \triangleleft G$ ,  $G/H$  abélien  $\Leftrightarrow D(G) \subset H$

1°/

$$D(G) = \{ z \in G \mid z = a_1^{e_1} \dots a_n^{e_n} \quad a_i = x_i y_i x_i^{-1} y_i^{-1} \text{ et } e_i = \pm 1 \}$$

$$u(a_1^{e_1} \dots a_n^{e_n}) = u(a_1)^{e_1} \dots u(a_n)^{e_n}$$

$$\text{et } u(a_i) = u(x_i) u(y_i) u(x_i)^{-1} u(y_i)^{-1} \in D(G)$$

d'où  $u(D(G)) \subset D(G)$

2°/

$$G/H \text{ abélien} \Leftrightarrow \forall x, y \in G \quad \cancel{xH \times yH = (xy)H = (yx)H} \\ xH \times yH = H(xy) = H(yx)$$

$$\Leftrightarrow xy(yx)^{-1} \in H$$

$$\Leftrightarrow \forall x, y \in G \quad xyx^{-1}y \in H \Leftrightarrow D(G) \subset H$$

CGFD

## Extension

Soit  $G$  un groupe. Les éléments embêtants sont ceux qui ne commutent pas avec les autres. On les réunit en un sous-groupe ("on les met dans le même sac") puis on fait le quotient de  $G$  par  $D(G)$  qui est distingué.

(voir  $D(G)$  invariant par tout automorphisme intérieur de  $G$ , cf d?)

L'embêtement a disparu : le groupe quotient est commutatif.

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/D(G) \\ \text{non abélien} & & \text{abélien} \end{array}$$

---

## Feuille N° 5

× 1<sup>re</sup> Résoudre dans  $\mathbb{Z}$  le système :

$$\begin{cases} 4x + y + 3z - t = 6 \\ x + y + 3z + 2t = -3 \\ 2x - 3y + 2z - 3t = 3 \end{cases}$$

✓ 2<sup>de</sup> Trouver toutes les matrices à coefficients entiers de la forme  $\begin{pmatrix} 1 & 4 & * \\ 2 & 5 & * \\ 1 & 6 & * \end{pmatrix}$  et de déterminant 1

✓ 3<sup>de</sup> Trouver les matrices diagonales équivalentes aux matrices suivantes :

$$\begin{pmatrix} 0 & 2 & 4 & -1 \\ 6 & 12 & 14 & 5 \\ 0 & 4 & 14 & -1 \\ 10 & 6 & -4 & 11 \end{pmatrix} \quad \begin{pmatrix} 0 & 6 & -9 & -3 \\ 12 & 24 & 9 & 9 \\ 30 & 42 & 45 & 27 \\ 66 & 78 & 81 & 63 \end{pmatrix} \quad \text{etc...}$$

× 4<sup>de</sup> On considère le morphisme  $f: \mathbb{Z}^3 \rightarrow \mathbb{Z}^4$  dont la matrice, dans les bases canoniques est  $\begin{pmatrix} 2 & 0 & 1 \\ -1 & 2 & 4 \\ 3 & 6 & 3 \\ 1 & -3 & 1 \end{pmatrix}$   
Identifier  $\ker f$  et  $\text{Im} f$  (Trouver leur rang) et calculer le conoyau de  $f$ .

x 5<sup>o</sup> Soit  $G$  le groupe additif des polynômes à coefficients entiers de degré  $\leq 1$ . Montrer que le quotient de  $G$  par le sous-groupe engendré par les polynômes  $8X+21$ ,  $4X+9$ ,  $5X^2$ ,  $7X^3+7X^4$  est  $\cong \mathbb{Z}/420\mathbb{Z} \times \mathbb{Z}$ .

x 6<sup>o</sup> Soit  $f: \mathbb{Z}^2 \rightarrow \mathbb{Z}^2$  de matrice  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ; donner une CNS sur  $a, b, c, d$  pour que  $\mathbb{Z}^2 / \text{Im } f$  soit cyclique. préciser la structure de  $\mathbb{Z}^2 / \text{Im } f$  si  $f$  a pour matrice  $\begin{pmatrix} 2 & 4 \\ -6 & 0 \end{pmatrix}$ . (Partiel 78)

x 7<sup>o</sup> Trouver un générateur de  $V(\mathbb{Z}/17\mathbb{Z})$ ; combien y en a-t-il?

AR x 8<sup>o</sup> Déterminer les nombres  $n$  pour lesquels  $V(\mathbb{Z}/n\mathbb{Z})$  est isomorphe à  $(\mathbb{Z}/n\mathbb{Z})^k$ .

x 9<sup>o</sup> Montrer que l'équation  $(n^2+1)x - (n+1)y = 1$  n'est résoluble dans  $\mathbb{Z}$  que si  $n$  est pair. Quelles sont ses solutions?

x 10<sup>o</sup> Montrer que pour tout entier  $n$ ,  $2730$  divise  $n^{13} - n$ .

(1) on trouve, après réductions par opérations élémentaires

$$\begin{array}{c}
 \begin{array}{ccc|ccc}
 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
 0 & 1 & 0 & 0 & 8 & 1 & 0 \\
 0 & 0 & 1 & 0 & 176 & 22 & 1
 \end{array} \\
 \hline
 \begin{array}{cccc}
 1 & 2 & -10 & -27 \\
 0 & 1 & 15 & 41 \\
 -3 & -4 & 9 & 24 \\
 0 & 5 & -16 & -43
 \end{array}
 \end{array}
 \quad \begin{array}{c}
 \leftarrow T^{-1} \\
 \\
 \\
 \\
 \end{array}$$

$M'$   $S$

$$\begin{array}{ccc}
 X \in \mathcal{B} & \xrightarrow{M} & \mathcal{A} \\
 \uparrow S & & \uparrow T \\
 \mathcal{B}' & & \mathcal{A}' \\
 X' & & Y'
 \end{array}$$

$M' = T^{-1}MS$  est donné dans la matrice.

$$\begin{array}{ll}
 Y \text{ donné} & Y' = T^{-1}Y \\
 X \text{ cherché} & X = SX'
 \end{array}
 \quad \begin{array}{l}
 T^{-1} \text{ lu sur la matrice} \\
 S \quad \quad \quad
 \end{array}$$

d'où  $Y' = \begin{pmatrix} 6 \\ 45 \\ 993 \end{pmatrix}$

et

$$\left\{ \begin{array}{l} X' = \begin{pmatrix} 6 \\ 45 \\ 993 \\ t \end{pmatrix} \\ \forall t \in \mathbb{R} \end{array} \right. \Rightarrow X = SX' = \begin{pmatrix} -9834 - 27t \\ 14945 + 41t \\ 8739 + 24t \\ -15713 - 43t \end{pmatrix}$$

On peut simplifier ce résultat en posant  $v = -364 - u$ .

on trouve;

$$x = \begin{pmatrix} -6 + 27v \\ 21 - 41v \\ 3 - 24v \\ -61 + 43v \end{pmatrix}$$

$$v \in \mathbb{Z}$$

④  $f: \mathbb{Z}^3 \rightarrow \mathbb{Z}^4$

$$\begin{pmatrix} 2 & 0 & 1 \\ -1 & 2 & 4 \\ 3 & 6 & 3 \\ 1 & -3 & 1 \end{pmatrix} = M$$

$\text{Im} f \subset \mathbb{Z}^4 \Rightarrow \text{Im} f = \text{sous-groupe libre de rang } \leq 4$

$\text{Ker} f \subset \mathbb{Z}^3 \Rightarrow \text{Ker} f = \text{ " " " rang } \leq 3$

$$\begin{pmatrix} 1 & 0 & 2 \\ 4 & 2 & -1 \\ 3 & 6 & 3 \\ 1 & -3 & 1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 4 & 2 & -9 \\ 3 & 6 & -3 \\ 1 & -3 & -1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & -9 \\ 0 & 6 & -3 \\ 0 & -3 & -1 \end{pmatrix}$$

$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 15 \\ 0 & 0 & 29 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 29 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \text{ est équivalente à } M.$$

Reste à trouver ce que représente cette matrice pour  $\text{Ker} f$  et  $\text{Im} f$

a.b.  $\mathbb{Z}^3 \xrightarrow{f} \mathbb{Z}^4$  ancienne base

$\downarrow \quad \downarrow$

n.b.  $\mathbb{Z}^3 \xrightarrow{f} \mathbb{Z}^4$  nouvelle base

$(e_1, e_2, e_3) \quad (b_1, b_2, b_3, b_4)$

Dans les nouvelles bases :  $f(x_1 e_1 + x_2 e_2 + x_3 e_3) = x_1 b_1 + x_2 b_2 + x_3 b_3$

$\text{Im} f$  est engendré par le système  $\{b_1, b_2, b_3\}$ , et est isomorphe à  $\mathbb{Z}^3$ .

$$\boxed{\text{Im} f \simeq \mathbb{Z}^3} \simeq \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times 0\mathbb{Z} \text{ en effet } \text{Im} f = \left\{ \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} / \exists u, v, w / \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} = \begin{pmatrix} u \\ v \\ w \\ 0 \end{pmatrix} \right\}$$

(c.à.d., est de rang 3)

$$\downarrow \quad \downarrow$$

$$(u, v, w, 0) \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times 0\mathbb{Z}$$

$$\text{Ker} f = \{ x_1 e_1 + x_2 e_2 + x_3 e_3 / x_1 b_1 + x_2 b_2 + x_3 b_3 = 0 \}$$

$\Leftrightarrow$

$$x_1 = x_2 = x_3 = 0$$



Donc  $\boxed{\text{Ker } f = \{0\}}$

$\text{Coker } f \doteq \mathbb{Z}^4 / \text{Im } f$

$\mathbb{Z}^4 / \text{Im } f \cong \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$  *pas évident*

$\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$

$\cong \mathbb{Z}$

$\mathbb{Z} / \mathbb{Z} \times \mathbb{Z} / \mathbb{Z} \times \mathbb{Z} / \mathbb{Z} \times \mathbb{Z} / \mathbb{Z}$  *voir [2]*

$\cong \mathbb{Z}$

Autre façon :

Présentation d'un sous-groupe (cf cours)

$\mathbb{Z}^4 / \text{Im } f \xrightarrow{\sim}$

⚠ Gn a' :  
en général

$H \cong H' \not\Rightarrow G/H \cong G/H'$

[1]

[2] Prendre, par exemple

$\mathbb{Z}^2 / d_1 \mathbb{Z} \times d_2 \mathbb{Z} \xrightarrow{\varphi \sim} \mathbb{Z} / d_1 \mathbb{Z} \times \mathbb{Z} / d_2 \mathbb{Z}$

$(\vec{x}, \vec{y}) \mapsto (\bar{x}_{d_1}, \bar{y}_{d_2})$

⑤  $P_1(x) = 8x + 21$

$P_2(x) = 4x + 9$

$P_3(x) = 5x^2$

$P_4(x) = 7x^3 + 7x^4$

$G$  est un groupe  $\alpha$ -galtf et, dans la base canonique  $(1, x, x^2, x^3, x^4)$  on a:

$\beta : G \rightarrow G$

$$\beta = \begin{pmatrix} 21 & 9 & 0 & 0 & 0 \\ 8 & 4 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & 7 & 0 \\ 0 & 0 & 0 & 7 & 0 \end{pmatrix}$$

(dans la base canonique)

On a  $\text{Im } \beta =$  groupe engendré par  $(P_1, P_2, P_3, P_4)$ , par construction.

La question revient à déterminer, à un isomorphisme près, le conoyau de  $\beta$ :

$\text{Coker } \beta = G / \text{Im } \beta \simeq ?$

● fait comme dans l'exercice précédent.

$$\beta \rightsquigarrow \begin{pmatrix} 5 & 1 & 0 & 0 \\ 8 & 4 & 0 & 0 \\ 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 7 \\ 0 & 0 & 0 & 7 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 5 & 0 & 0 \\ 4 & 8 & 0 & 0 \\ 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 7 \\ 0 & 0 & 0 & 7 \end{pmatrix}$$

$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -12 & 0 & 0 \\ 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 7 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

(remarque: ce n'est pas la base canonique, car  $d_i \neq d_{i+1}$  !)

Donc  $\text{Im } \beta \simeq \mathbb{Z} \times \mathbb{Z}_{12} \times 5\mathbb{Z} \times 7\mathbb{Z} \times 0\mathbb{Z}$

$$G/\text{Im } \beta \simeq \mathbb{Z}^5 / \mathbb{Z} \times \mathbb{Z}_{12} \times 5\mathbb{Z} \times 7\mathbb{Z} \times 0\mathbb{Z}$$

important.

$$\simeq \underbrace{\mathbb{Z}/\mathbb{Z}}_{\text{triv}} \times \mathbb{Z}/_{12}\mathbb{Z} \times \mathbb{Z}/_5\mathbb{Z} \times \mathbb{Z}/_7\mathbb{Z} \times \underbrace{\mathbb{Z}/_0\mathbb{Z}}_{\mathbb{Z}}$$

(voir cours)

$$\boxed{G/\text{Im } \beta \simeq \mathbb{Z}/_{420}\mathbb{Z} \times \mathbb{Z}}$$

(NB: on généralise  $\mathbb{R}G$   
 $H, F \subset G$   
 $H \simeq F \not\Rightarrow G/H \simeq G/F$ )

Remarque :

Si l'on veut la "forme canonique" de la matrice de  $\beta$  :

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -12 & 0 & 0 \\ 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 7 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{\text{problème}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -12 & 0 & 0 \\ 0 & 0 & 5 & 15 \\ 0 & 0 & 0 & 7 \\ 0 & 0 & 0 & 0 \end{pmatrix} \leftarrow \text{on change un 0 en un nbre } \neq 0$$

$$\sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -12 & 0 & 0 \\ 0 & 0 & 5 & 1 \\ 0 & 0 & 0 & 7 \\ 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 5 & 1 \\ 0 & -12 & 0 & 0 \\ 0 & 0 & 0 & 7 \\ 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 5 & 0 \\ 0 & 0 & 0 & -12 \\ 0 & 7 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -12 \\ 0 & 7 & -35 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -12 \\ 0 & 0 & -35 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 420 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

⑥  $f: \mathbb{Z}^2 \rightarrow \mathbb{Z}^2$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  CNS  $\mathbb{Z}^2 / \text{Im} f$  cyclique.

On sait que  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \sim \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}$  où  $\begin{cases} d_1 \\ d_2 \end{cases}$   
où  $d_1 | d_2$

d'où  $\text{Coker} f = \mathbb{Z}^2 / \text{Im} f = \mathbb{Z}^2 / d_1 \mathbb{Z} \times d_2 \mathbb{Z} \simeq \mathbb{Z} / d_1 \mathbb{Z} \times \mathbb{Z} / d_2 \mathbb{Z}$

\* Si  $d_1 d_2 \neq 0$   $\mathbb{Z}^2 / \text{Im} f$  est cyclique si  $\text{O}(d_1, d_2) = 1$  (Théorème Chinois)

Or  $d_1 | d_2 \Rightarrow \text{O}(d_1, d_2) = 1$  si  $d_1 = 1$

\* Si  $d_1 = 0 = d_2$ , alors  $f = \vec{0}$  et  $\text{Im} f = \{0\} \Rightarrow \mathbb{Z}^2 / \text{Im} f \simeq \mathbb{Z}^2$  ~~cyclique~~ non cyclique.

\* Si  $d_2 = 0$  et  $d_1 \neq 0$  (l'autre cas est impossible car  $d_1 | d_2$ )

$\mathbb{Z}^2 / \text{Im} f \simeq \mathbb{Z} / d_1 \mathbb{Z} \times \mathbb{Z}$

si il était cyclique, il serait de la forme  $\mathbb{Z} / d \mathbb{Z}$  ou  $\mathbb{Z}$ .

Il ne peut être isomorphe à  $\mathbb{Z} / d \mathbb{Z}$  car  $\mathbb{Z} / d \mathbb{Z}$  est fini.

Il ne peut être isomorphe à  $\mathbb{Z}$  car il possède des éléments d'ordre fini dans  $\mathbb{Z} / d_1 \mathbb{Z}$  si  $d_1 \neq 1$

Ainsi  $\begin{cases} d_1 = 1 & \mathbb{Z}^2 / \text{Im} f \text{ est cyclique} \\ d_1 \neq 1 & \mathbb{Z}^2 / \text{Im} f \text{ non cyclique} \end{cases} \quad (d_2 = 0)$

Conclusion :

$$\mathbb{Z}^2/\mathcal{O}_{mf} \text{ est cyclique si } d_1 = -1 = \Delta(a, b, c, d)$$

Application

$$\begin{pmatrix} 2 & 4 \\ -6 & 0 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 \\ -6 & 12 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 \\ 0 & 12 \end{pmatrix}$$

$$\Delta(2, 12) = 2 \neq 1 \Rightarrow \mathbb{Z}^2/\mathcal{O}_{mf} \text{ n'est pas cyclique.}$$

$$\text{Mais } \mathbb{Z}^2/\mathcal{O}_{mf} \simeq \mathbb{Z}^2/_{2\mathbb{Z} + 12\mathbb{Z}} \simeq \mathbb{Z}/_2\mathbb{Z} \times \mathbb{Z}/_{12}\mathbb{Z}$$

Si on décompose en composantes primaires le sous-groupe  $\mathbb{Z}^2/\mathcal{O}_{mf}$ , on trouve :

$$\mathbb{Z}^2/\mathcal{O}_{mf} \simeq \mathbb{Z}/_2\mathbb{Z} \times \mathbb{Z}/_{3 \times 4}\mathbb{Z} \simeq \underbrace{(\mathbb{Z}/_2\mathbb{Z} \times \mathbb{Z}/_4\mathbb{Z})}_{G(2)} \times \underbrace{\mathbb{Z}/_{3}\mathbb{Z}}_{G(3)}$$

⑦  $\mathcal{U}(\mathbb{Z}/_{17}\mathbb{Z})$  est un groupe multiplicatif abélien. Il est cyclique car  $\mathbb{Z}/_{17}\mathbb{Z}$  est un corps fini, à 16 éléments.

Quels sont les ordres possibles : 1, 2, 4, 8, 16

$$\mathcal{U}(\mathbb{Z}/_{17}\mathbb{Z}) = \{ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 \}$$

$n$	$\omega(n)$	
1	1	
2	8	car $2^2 = 4$ et $(-1)^2 = 1$ donc c'est 16.
3	16	car $3^2 = 9$ , $3^3 = 27 \equiv 10$ , $3^4 = 81 \equiv -4$ donc $\omega(3) \neq 2$ et $4$ . et $3^8 = (3^4)^2 = 16 \equiv 1$ donc $\omega(3) = 16$ .

Le nombre de générateurs de  $U(\mathbb{Z}/_{17}\mathbb{Z})$  est égal au nbre de générateurs de  $\mathbb{Z}/_{16}\mathbb{Z}$ , c.à.d  $\varphi(16) = \varphi(2^4) = 2^3 = 8$

Trouvons les autres générateurs.

On a :  $U(\mathbb{Z}/_{17}\mathbb{Z}) = \{ 3^k \mid 0 \leq k \leq 16 \}$

et :  $3^k$  engendre  $U(\mathbb{Z}/_{17}\mathbb{Z}) \Leftrightarrow \Delta(k, 16) = 1$

en effet :

$$\begin{array}{ccc} \varphi : \mathbb{Z}/_{16}\mathbb{Z} & \xrightarrow{\sim} & U(\mathbb{Z}/_{17}\mathbb{Z}) \\ k & \longmapsto & 3^k \end{array}$$

Cela provient de  
(3 générateur de  $U(\mathbb{Z}/_{17}\mathbb{Z})$ )  
1 générateur de  $\mathbb{Z}/_{16}\mathbb{Z}$ )

et pour trouver tous les générateurs de  $U(\mathbb{Z}/_{17}\mathbb{Z})$ , il suffit et il faut de trouver les générateurs de  $\mathbb{Z}/_{16}\mathbb{Z}$ , c.à.d les  $k \in \mathbb{Z}/_{16}\mathbb{Z}$  tels que

$\Delta(k, 16) = 1$

$\Downarrow$   
 $k$  impair.

Les huit générateurs de  $U(\mathbb{Z}/_{17}\mathbb{Z})$  sont

$$\{ \overset{3}{3}, \underset{11}{10}, \overset{5}{5}, \underset{11}{11}, 14, 7, 12, 6 \}$$

Moralité: quand on a trouvé 1 générateur, on en déduit tous les autres.

$$(8) \quad U(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/2\mathbb{Z})^k \quad (1)$$

Seit

$$n = 2^x \prod p_i^{x_i} \quad p_i \neq 2$$

la décomposition de  $n$  en facteurs premiers.

Le théorème chinois nous donne  $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/2^a\mathbb{Z} \times \prod_{i=1}^r \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$  (isomorphisme d'anneaux)

et (on l'a déjà utilisé)  $u(\mathbb{Z}/n\mathbb{Z}) \underset{(\hat{m} \text{ isomorphisme})}{\simeq} u(\mathbb{Z}/2^a\mathbb{Z}) \times \prod u(\mathbb{Z}/p_i^{a_i}\mathbb{Z})$

4) Sei  $\alpha = 0$

$$\text{Def } u(\mathbb{Z}/n\mathbb{Z}) \simeq \prod_i \mathbb{Z} / p_i^{\alpha_i-1} (p_i-1) \mathbb{Z}$$

(voir cours)

$u(\mathbb{Z}/p_i\mathbb{Z})$  cyclique, si  $p_i \neq 2$   
 $p_i$  premier

2) Si  $\alpha = 1$

$$u(\mathbb{Z}/n\mathbb{Z}) \simeq \underbrace{u(\mathbb{Z}/2\mathbb{Z})}_{\{1\}} \times \prod_i \mathbb{Z}/_{p_i^{a_i}(p_i-1)\mathbb{Z}}$$

$$12 \quad \prod_i \mathbb{Z} / p_i^{\alpha_i-1} (p_i-1) \mathbb{Z}$$

6

3) Si  $\alpha = 2$

Comme  $u(\mathbb{Z}/4\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ , on obtient

$$u(\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \times \prod_i \mathbb{Z}/_{p_i^{\alpha_i-1}(p_i-1)}\mathbb{Z}$$

4) Si  $\alpha > 2$

$$u(\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/_{2^{\alpha-2}}\mathbb{Z} \times \prod_i \mathbb{Z}/_{p_i^{\alpha_i-1}(p_i-1)}\mathbb{Z}$$

Revenons à notre second terme :

Dans  $(\mathbb{Z}/2\mathbb{Z})^k$ , tout élément doit être d'ordre 2 au plus.

Si  $\alpha \geq 4$ ,  $\exists$  ~~est~~, dans  $\mathbb{Z}/_{2^{\alpha-2}}\mathbb{Z}$ , des éléments d'ordre supérieur à 2

$$\Downarrow \\ 2^{\alpha-2} \geq 2^2 > 2$$

ainsi, si  $\alpha \geq 4$ , il n'y a pas de solution pour (1) Le seul cas intéressant pour le 4) est que  $\alpha = 3$

4\*) Si  $\alpha = 3$

$$u(\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \prod_i \mathbb{Z}/_{p_i^{\alpha_i-1}(p_i-1)}\mathbb{Z}$$

Le premier facteur, dans les trois cas, est toujours de la forme  $(\mathbb{Z}/2\mathbb{Z})^k$  où  $k = 0, 1, 2$ .



Passons au 2-facteur :  $\alpha_i \geq 2 \Rightarrow p_i \mid p_i^{\alpha_i-1}(p_i-1)$

donc  $p_i$  divise le cardinal de  $\mathbb{Z}/_{p_i^{\alpha_i-1}(p_i-1)}\mathbb{Z}$

$\Downarrow$

$\exists n \in \mathbb{Z}/_{p_i^{\alpha_i-1}(p_i-1)}\mathbb{Z}$  d'ordre  $p_i \geq 2$ .

Mais il n'y a pas de solution à (1)

Donc  $\alpha_i = 1$ . ( $\forall i \in I$ )

les seconds facteurs sont de la forme  $\mathbb{Z}/_{(p_i-1)}\mathbb{Z}$ . Il existe  $n \in \mathbb{Z}/_{(p_i-1)}\mathbb{Z}$  ayant pour ordre  $p_i-1$ . Donc, il existe un élément d'ordre  $p_i-1$  dans  $U(\mathbb{Z}/_n\mathbb{Z})$  qui ne peut contenir que des éléments d'ordre  $\leq 2$ . Donc  $p_i-1 \leq 2 \Leftrightarrow \underline{p_i = 3}$  (car  $p_i \neq 2$ , si  $p_i = 0$ , on n'écrit pas le nbre premier dans la décomposition de  $n$  en nbres premiers).

Donc

$$n = 2^\alpha \quad 3 \times 2^\alpha \quad (\alpha \leq 3)$$

Pour

c.à.d.  $n \in \{1, 2, 3, 4, 6, 8, 12, 24\}$

$k \in \{0, 0, 1, 1, 1, 2, 2, 3\}$

construit à partir  
de  $\varphi(n) = 2^k$

$\Uparrow$

$$U(\mathbb{Z}/_n\mathbb{Z}) \simeq (\mathbb{Z}/_2\mathbb{Z})^k$$

Remarque :  $U(\mathbb{Z}/_n\mathbb{Z}) \simeq (\mathbb{Z}/_2\mathbb{Z})^k \Rightarrow \varphi(n) = 2^k$ , réciproque fautive comme vous pouvez vous attendre.

⑨  $(n^2+1)x - (n+1)y = 1$  résoluble dans  $\mathbb{Z} \Leftrightarrow n$  est pair

- Si  $n$  est impair,  $n^2+1$  et  $n+1$  sont pairs, absurde :  $S = \emptyset$  (l'ensemble des solutions)
- Supposons maintenant que  $n$  soit pair.

L'équation est résolublessi  $\Delta(n^2+1, n+1) = 1$ . Montrons donc que  $n$  pair  $\Rightarrow \Delta(n^2+1, n+1) = 1$

Soit  $d$  diviseur commun à  $n+1$  et  $n^2+1$

$$\bullet \quad \left. \begin{array}{l} \text{Or } d \mid (n+1)^2 = n^2 + 2n + 1 \text{ donc } d \mid 2n \\ d \mid 2(n+1) \end{array} \right\} \Rightarrow d \mid 2 \Rightarrow d \in \{\pm 1, \pm 2\}.$$

$d = \pm 2$  impossible car  $n+1$  impair.

Donc  $d = \pm 1$ .

Donc  $\Delta(n^2+1, n+1) = 1$ . L'équation est résoluble dans  $\mathbb{Z}$ .

\* Résolution  $(n^2+1)x - (n+1)y = 1$

● Sol. particulière:

$n$  pair  $n = 2q$ . Supposons  $n \geq 2$ .

$$\text{Or } (n^2+1) = (n+1)(n-1) + 2 \quad 0 \leq 2 < n+1$$

$$n+1 = 2q+1$$

$$\text{d'où } (n^2+1)(-q) - (n+1)[-1 - q(n-1)] = 1 \quad (1)$$

Résolution

$$\begin{cases} (n^2+1)x - (n+1)y = 1 \\ (n^2+1)x_0 - (n+1)y_0 = 1 \end{cases}$$

$$(n^2+1)(x_0 - x) = (n+1)(y_0 - y) \quad \text{et } \Delta(n+1, n^2+1) = 1 \quad (\text{cf (1)})$$

Done

$$\begin{cases} x_0 - x = (n+1)k \\ y_0 - y = (n^2+1)k \end{cases} \quad k \in \mathbb{Z}$$

$$\begin{cases} x = x_0 - (n+1)k \\ y = y_0 - (n^2+1)k \end{cases} \quad k \in \mathbb{Z}$$

⑩ a)  $\forall n \in \mathbb{Z} \quad 2730 \mid n^{13} - n$

b)  $\forall n, m \in \mathbb{Z} \quad 56786730 \mid nm(n^{60} - m^{60}) \quad (\text{Capes})$

a) 
$$\begin{aligned} n^{13} - n &= n(n^{12} - 1) = n(n^6 + 1)(n^6 - 1) \\ &= n(n^6 + 1)(n^3 + 1)(n - 1)(n^2 + n + 1) \end{aligned}$$

Remarque :  $d \mid k \Rightarrow (n^d - 1) \mid (n^k - 1) \quad (\forall n \in \mathbb{N}^*)$

Preuve: On pose  $k = kd$ . Alors  $(n^k - 1) = (n^{kd} - 1) = (n^d - 1)(\dots)$

•

On a  $n^{13} - n = n(n^{12} - 1)$

Cherchons les diviseurs de 12 :  $\mathcal{D}(12) = \{1, 2, 3, 4, 6, 12\}$

Ainsi  $\{n-1, n^2-1, n^3-1, n^4-1, n^6-1, n^{12}-1\}$  divisent  $n^{13}-n$

On a

2730	2
1365	5
273	3
91	7
13	13
1	

Remarquons que :  $\{1, 2, 3, 4, 6, 12\} = \text{diviseurs de } 12$   
 $E = \{2, 3, ?, 5, 7, 13\} = \text{décomp. de } 2730 \text{ en nbres premiers}$

Le théorème de Fermat :  $n^{p-1} \equiv 1 \pmod{p} \quad \left\{ \begin{array}{l} \Delta(n, p) = 1 \\ p \text{ premier} \end{array} \right.$

preuve:  $\#U(\mathbb{Z}/p\mathbb{Z}) = p-1$   
 si  $n \neq 0$ ,  $n^{p-1} = 1$  dans  $\mathbb{Z}/p\mathbb{Z}$ . (Facile)  
 $\uparrow$   
 $n \neq kp \quad n^{p-1} \equiv$

$$\forall p \in E, \quad n^p \equiv n \pmod{p}$$

$\Leftrightarrow$

$$n^p - n \equiv 0 \pmod{p} \quad (1) \text{ vraie si } \Delta(n, p) = 1$$

$$n(n^{p-1} - 1) \equiv 0 \pmod{p} \quad (1') \text{ vraie } \forall n, \text{ cette fois-ci}$$

Or  $p-1$  est un diviseur de 12, donc  $n^{p-1} - 1 \mid n^{12} - 1$

$\Downarrow$

$$n^p - n \mid n^{13} - n \quad (2)$$

Traduisons :

$$\left. \begin{array}{l} (1) \Rightarrow p \mid n^p - n \\ (2) \Rightarrow n^p - n \mid n^{13} - n \end{array} \right\} \Rightarrow p \mid n^{13} - n \text{ c'est } \forall p \in E$$

$\Downarrow$

$\infty$

$$2730 \mid n^{13} - n$$

b)

diviseurs de 60 =  $\{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$

fact. premiers =  $\{2, 3, 5, 7, 11, 13, 31, 61\}$

$$\begin{array}{c} d \\ \downarrow \\ d+1 = p \end{array}$$

Mais le problème est un peu différent.

$$\text{Si } d \mid 60 \Rightarrow n^d - m^d \mid n^{60} - m^{60}$$

$$p = d+1 \quad \left\{ \begin{array}{l} n^d \equiv 1 \pmod{p} \text{ si } \Delta(p, n) = 1 \\ m^d \equiv 1 \pmod{p} \text{ si } \Delta(p, m) = 1 \end{array} \right.$$

d'où  $n^d - m^d \equiv 0 \pmod{p} \Rightarrow p \mid n^d - m^d \Rightarrow p \mid nm(n^{d-1} - m^{d-1})$

Donc, si  $\delta(p, n) = \delta(p, m) = 1$ , alors  $p \mid nm(n^{d-1} - m^{d-1})$

Si, par exemple  $\delta(p, n) = 1 \Rightarrow p \mid n \Rightarrow p \mid nm(n^{d-1} - m^{d-1})$

c'est plus rapide

Dans tous les cas,  $p \mid nm(n^{d-1} - m^{d-1})$

$\forall p$  facteur premier intervenant dans la déc. de 56 786 730

Donc  $56\,786\,730 \mid nm(n^{60} - m^{60})$

Q.E.D.

## Feuille N° 6

- × 1° Soit  $k$  un corps à  $p^n$  éléments ( $p$  premier,  $n \in \mathbb{N}$ ); on désigne par  $F$  l'ensemble des applications de  $k$  dans lui-même. Soit  $\phi: k[x] \rightarrow F$  qui associe à un polynôme  $f$  la fonction polynôme correspondante.

Montrer que  $\ker \phi$  est l'idéal de  $k[x]$  engendré par  $X^{p^n} - X$ .

En déduire que  $\phi$  est surjective.

- × 2° Soit  $P \in \mathbb{R}[x]$  un polynôme tel que pour tout  $t \in \mathbb{R}$ ,  $P(t) \geq 0$ . Montrer qu'il existe deux polynômes  $R$  et  $S$  de  $\mathbb{R}[x]$  tels que
- $P = R^2 + S^2$ .

- × 3° Trouver les polynômes  $P$  à coefficients réels vérifiant
- $$P(x^2) = P(x) P(x+1).$$

- × 4° Soit un polynôme  $P(x) = x^3 - x - 1$ . Combien possède-t-il de racines réelles ? Soit  $\omega$  une racine réelle ; montrer que  $\omega \notin \mathbb{Q}$ . Montrer que  $\{1, \omega, \omega^2\}$  est une partie libre du  $\mathbb{Q}$ -espace vectoriel  $\mathbb{R}$ .

- × 5° Soit  $E$  l'espace vectoriel des polynômes réels (!) de

degré inférieur ou égal à  $n$ . Soit  $T$  l'application de  $E$  dans  $E$  définie par  $T(f) = g$  où  $g(x) = f(x+1) - f(x)$ .

Que pouvez-vous dire de  $T$  ?

x 6° Soit  $ax^2 + bx + c = 0$  une équation dans laquelle  $a, b, c$  sont entiers et  $a$  et  $c$  non nuls. Démontrez que si une racine est rationnelle, alors l'un au moins des coefficients est pair.

x 7° Soient  $a, b, c, d$  des entiers non nuls.

a) Montrez que  $a^3 + b^3 + c^3 \equiv 0 \pmod{7} \Rightarrow abc \equiv 0 \pmod{7}$ .

b) Montrez que si  $a^3 + b^3 + c^3 + d^3 \equiv 0 \pmod{7}$ , on n'a pas nécessairement  $abcd \equiv 0 \pmod{7}$ .

8° Résolvez dans  $\mathbb{Z}$  l'équation  $x^2 + y^2 = z^2$ . Montrez que  $x^4 + y^4 = z^4$  n'a pas de solution dans  $\mathbb{Z}$ .

9° Trouvez les  $p$ -composants de  $\mathbb{Z}/_{16\mathbb{Z}}$ ,  $\mathbb{Z}/_{24\mathbb{Z}}$ ,  $\mathbb{Z}/_{n\mathbb{Z}}$ .

10° Trouvez les  $p$ -composants de  $G = \mathbb{Z}/_{12\mathbb{Z}} \times \mathbb{Z}/_{15\mathbb{Z}} \times \mathbb{Z}/_{10\mathbb{Z}}$ .

x 11° Soit  $G$  un groupe commutatif d'ordre  $n$ . Montrez que si  $n = \prod_i p_i$  ( $p_i$  premier et  $i \neq j \Rightarrow p_i \neq p_j$ )  $G$  est un groupe cyclique. Exemple?

6.02.79



$$(3) P \in \mathbb{R}[X]$$

$$P(X^2) = P(X)P(X+1) \quad (1)$$

$$1) P(X) = 0 \Leftrightarrow a \Rightarrow a = a^2 \Rightarrow a = 1 \text{ ou } 0$$

2)  $P(X) \neq 0$ , th. de d'Alembert  $\Rightarrow$  Soit  $\alpha$  une racine de  $P(X)$ . Alors  $\alpha^2$  aussi.

$$\text{Pro} \left| \begin{array}{l} \alpha \text{ racine} \Rightarrow \alpha^{2^n} \text{ racine } (n \in \mathbb{N}) \\ \alpha \text{ racine} \Rightarrow (\alpha-1)^2 \text{ racine} \end{array} \right.$$

$$\text{Pro} \left| \begin{array}{l} \alpha \text{ racine} \neq 0 \\ \neq 1 \end{array} \Rightarrow \alpha^{2^n} \neq \alpha^{2^k} \text{ si } k \neq n \right.$$

En effet  $\exists k, n / \alpha^{2^n} = \alpha^{2^k} \Rightarrow |\alpha|^{2^n - 2^k} = 1 \Rightarrow |\alpha| = 1$

Ainsi : les seules racines de  $P$  sont 0, 1 ou  $\alpha \in \mathbb{C}$  tel que  $|\alpha| = 1$ .

On remarque que, si  $\alpha \in \mathbb{C} \setminus \{0, 1\}$   $|\alpha| = 1$ . Posons  $\alpha = e^{i\theta}$ .

Alors  $(e^{i\theta} - 1)^2$  est racine, donc  $|e^{i\theta} - 1| = 1 \Rightarrow (\cos \theta - 1)^2 + \sin^2 \theta = 1$

$$\Rightarrow 2 - 2\cos \theta = 1$$

$$\Rightarrow 2\cos \theta = 1 \Rightarrow \cos \theta = \frac{1}{2}$$

$$\Rightarrow \left\{ \begin{array}{l} \theta = \frac{\pi}{3} [2\pi] \\ \text{ou} \\ \theta = -\frac{\pi}{3} [2\pi] \end{array} \right. \quad (1)$$

Mais aussi  $(e^{i2\theta} - 1)^2$  est racine. Les m-calculs donnent

$$\left\{ \begin{array}{l} 2\theta = \frac{\pi}{3} [2\pi] \\ \text{ou} \\ 2\theta = -\frac{\pi}{3} [2\pi] \end{array} \right. \quad (2)$$

(1) et (2) sont incompatibles.

Donc les seules racines polynômes de  $P$  sont 0 ou 1, peut-être.

On écrit :

$$P(X) = k X^n (X-1)^m \quad \text{où } k^2 = k \Rightarrow k = 0 \text{ ou } k = 1$$

$$P(X^2) = k X^{2n} (X^2-1)^m$$

$$\begin{cases} P(X) = X^n (X-1)^m \\ P(X^2) = X^{2n} (X^2-1)^m \end{cases}$$

$$\text{or } P(X+1) = (X+1)^n (X)^m$$

$$\text{On doit avoir : } X^{2n} (X^2-1)^m = X^n (X-1)^m X^m (X+1)^n$$

$$X^{2n} (X-1)^m (X+1)^m = X^{n+m} (X-1)^m (X+1)^n \leftarrow \begin{array}{l} \text{décomposition} \\ \text{en polynômes irréducti-} \\ \text{-bles puisque de} \\ \text{degré 1.} \\ \text{Cette déc. est unique.} \end{array}$$

$\Downarrow$

$$\begin{cases} 2n = n+m \\ n = m \end{cases}$$

$\Downarrow$

$$n = m$$

Ainsi

$$\boxed{P(X) = X^n (X-1)^n}$$

Remarque sur le 4° : Autre méthode : résolution de  $X^3 - X - 1$

$$\boxed{X^3 + pX + q = 0 \quad (1)}$$

$$X = u + v \quad (2)$$

$$u^3 + v^3 + \underbrace{(3uv + p)}_{=0} (u+v) + q = 0$$

$$\text{Ponons } 3uv + p = 0 \quad (3)$$

$$\text{Alors (4) } \begin{cases} uv = -\frac{p}{3} \\ u^3 + v^3 = -q \end{cases}$$

$$\begin{cases} U = u^3 \\ V = v^3 \end{cases} \quad \text{d'où} \quad (4) \quad \begin{cases} UV = -\frac{p^3}{27} \\ U + V = -q \end{cases}$$

Rappel: Soit  $k$  un corps.  $\mathbb{Z} \xrightarrow{f} k$  morphisme de groupe pour  $+$   
 $1 \mapsto 1 = f(1)$

(on note 1 l'él. unité de  $k$  et 0 son él. neutre)

Il est aisé de vérifier que ce morphisme de groupe est aussi un morphisme d'anneau.  
 Considérons  $\text{Ker } f = p\mathbb{Z} \subset \mathbb{Z}$

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{f} & k \\ \pi \downarrow & & \uparrow i \\ \mathbb{Z}/p\mathbb{Z} & \xrightarrow[\tilde{f}]{\sim} & \boxed{\text{Im } f} \end{array}$$

c'est un sous-anneau de  $k$ , il est donc intègre.

Donc  $\mathbb{Z}/p\mathbb{Z}$  est un <sup>intègre</sup> ~~corps~~  $\Leftrightarrow p=0$  ou  $p$  premier.

On note  $p$  la caractéristique du corps  $k$ . Ainsi, si  $k$  est fini, alors  $p \neq 0$ .

$$\boxed{p = \text{car}(k) \quad k \text{ fini} \Rightarrow p \neq 0}$$

Pro | Si  $\text{Card } k < \infty$ , alors  $\text{Card } k = p^n$  ( $p$  premier et  $n \in \mathbb{N}$ )

$\text{Card } k < \infty$ . Soit  $p$  la caractéristique du corps  $k$

Alors  $k$  est un espace vectoriel sur  $\mathbb{Z}/p\mathbb{Z}$ , par  $\mathbb{Z}/p\mathbb{Z} \times k \rightarrow k$

$$(\lambda, x) \mapsto \underbrace{\tilde{f}(\lambda)}_n \underbrace{x}_x \in k$$

Comme il n'y a qu'un nbre fini de vecteurs dans  $k$ ,  $k$  sera un espace vectoriel de dimension finie sur  $\mathbb{Z}/p\mathbb{Z}$ . Et donc, si  $\dim k = n < \infty$ .

$$k \cong (\mathbb{Z}/p\mathbb{Z})^n \Rightarrow \boxed{\text{Card } k = p^n}$$

Pro | Si  $k$  est un corps fini, alors  $k$  est commutatif (Wedderburn)

(cf. Bouvier Richard)

①  $\#k = p^n \quad F = k^k$

$$\Phi: k[x] \rightarrow F$$

$$b \mapsto \Phi(b) \quad \text{où, si } b = \sum_{i=0}^n a_i x^i$$

$$\Phi(b)(\lambda) = \sum_{i=0}^n a_i \lambda^i \doteq b(\lambda)$$

Montrons que  $\ker \Phi = \{(x^{p^n} - x)b \mid b \in k[x]\}$

$\ker \Phi$  est un idéal.

Pro |  $b \in k[x]$   
 $\dim_k \frac{k[x]}{\underbrace{bk[x]}_{(b)}} = \deg b$

Preuve : laissée au lecteur.

On remarque, par exemple, que  $\mathbb{R}[x] / \underbrace{(x^2+1)\mathbb{R}[x]}_{(b)} \simeq \mathbb{C}$   
 $b \mapsto b(i)$

$\exists g \in k[X] / \text{Ker } \Phi = (g)$  (cf cours :  $K \text{ corps} \Rightarrow K[X] \text{ principal}$ )

et  $\deg g = \min \{ \deg f / f \neq 0 \text{ et } f \in \text{Ker } \Phi \}$

On constate que  $X^{p^n} - X \in \text{Ker } \Phi$  puisque :

$$\forall x \in k \quad \Phi(X^{p^n} - X)(x) = x^{p^n} - x = 0 \quad \text{car} \begin{cases} \text{si } x=0, \text{ c'est vrai.} \\ \text{si } x \neq 0, x \in k^\times \text{ et } \# k^\times = p^n - 1 \\ \text{donc } x^{p^n-1} = 1 \Rightarrow x^{p^n} = x \end{cases}$$

donc  $\Phi(X^{p^n} - X) = 0 \in k^k$

Ainsi  $(X^{p^n} - X) \subset \text{Ker } \Phi$ .

A retenir : si  $f \in \text{Ker } \Phi$ ,  $\deg f \geq p^n$ .

$f \in \text{Ker } \Phi \Leftrightarrow \forall x \in k \quad f(x) = 0$  donc  $f$  admet  $p^n$  racines,  
et donc  $\deg f \geq p^n$

En déduire que  $\Phi$  est surjective.

Eni, d'après la proposition rappelée :

$$\dim_k \frac{k[X]}{\text{Ker } \Phi} = p^n \quad \text{or} \quad \frac{k[X]}{\text{Ker } \Phi} \simeq \underbrace{\text{Im } \Phi}_{(1)} \subset F$$

$$(1) \text{ et } \left\{ \begin{array}{l} \underbrace{\text{Card } \frac{k[X]}{\text{Ker } \Phi}}_{\text{espace vectoriel}} = (\# k)^{p^n} = (p^n)^{p^n} \Rightarrow \text{Card Im } \Phi = (p^n)^{p^n} \\ \text{et Card } F = \underbrace{\# k}_{\substack{\uparrow \\ \text{car } F = k^k}} (p^n)^{p^n} \Rightarrow \text{Im } \Phi = F \end{array} \right.$$

Conséquence : dans un corps fini  $k$ , toute application de  $k$  dans lui-même est une application polynomiale.

Autre méthode.

$$\forall f \in \text{Ker } \Phi \quad f \neq 0 \quad \deg f \geq p^n \quad (\text{faute } f(n)=0 \quad \forall n \Rightarrow f \text{ admet } p^n \text{ racines})$$

$$\text{Soit } \text{Ker } \Phi = (h) \Rightarrow \deg h \geq p^n$$

$$\text{Donc } \frac{k[X]}{\text{Ker } \Phi} \simeq \text{Im } \Phi \subset F \quad (1)$$

$$\left. \begin{array}{l} \# k[X] = (p^n)^{\deg h} \\ \dim_{\mathbb{Q}} \frac{k[X]}{\text{Ker } \Phi} = \deg h \geq p^n \\ \# \end{array} \right\} \Rightarrow \left. \begin{array}{l} \# \text{Im } \Phi \geq (p^n)^{p^n} \\ \# \text{Im } \Phi \leq (p^n)^{p^n} \end{array} \right\} \Rightarrow \text{Im } \Phi = F \quad (1)$$

$$(2) \quad P \in \mathbb{R}[X] \quad \forall t \in \mathbb{R} \quad P(t) \geq 0 \quad (1)$$

$$\text{Montrer que : } \exists R, S \in \mathbb{R}[X] \quad / \quad P = R^2 + S^2$$

. Soit  $P$  qui vérifie (1).

Lemme : Si  $P(a) = 0$ , alors  $P(X) = (X-a)^{2\lambda} Q(X)$  avec  $Q(a) \neq 0$

$$\text{Si } P(X) = \underbrace{(X-a)^{2\lambda+1}}_{\text{pos de signe}} \underbrace{Q(X)}_{\text{pos de un signe constant au voisinage de } a} \quad Q(a) \neq 0. \Rightarrow (1) \text{ Faux. Absurde.}$$

pos de signe : pos de un signe constant au voisinage de  $a$ .

Soit  $P = Q \prod_{1 \leq i \leq p} (X - a_i)^{2n_i}$  avec  $Q(t) > 0 \quad \forall t \in \mathbb{R}$

Remarque:

$$\begin{aligned} (a^2 + b^2)(c^2 + d^2) &= a^2 c^2 + a^2 d^2 + b^2 c^2 + b^2 d^2 \\ &= (ac - bd)^2 + (ad + bc)^2 \end{aligned}$$

donc le produit de sommes de 2 carrés est une somme de 2 carrés.

$$P(X) = Q(X) \prod_{i=1}^p (X - a_i)^{2n_i} \quad \text{où } Q(t) > 0 \quad (t \in \mathbb{R})$$

Les racines de  $Q$  sont  $a_1, \dots, a_k, \bar{a}_1, \dots, \bar{a}_k$  (th. de d'Alembert).

Donc 
$$Q(X) = A \prod_{i=1}^k (X - a_i)(X - \bar{a}_i) = A \prod_{i=1}^k \underbrace{(X^2 - 2\operatorname{Re} a_i X + |a_i|^2)}_{X^2 - \alpha X + \beta}$$

$$X^2 - \alpha X + \beta = \left(X - \frac{\alpha}{2}\right)^2 - \frac{\alpha^2}{4} + \beta = \left(X - \frac{\alpha}{2}\right)^2 + \underbrace{\frac{4\beta - \alpha^2}{4}}_{> 0 \text{ (sinon, il existerait des rac. réelles)}}$$

Donc  $Q$  = somme de 2 carrés. On utilise la remarque un grand nombre de fois (récurrence finie), et l'on obtient bien  $Q = P^2 + 1$   $P = R^2 + S^2$

2<sup>e</sup> méthode

$$\begin{aligned} P \in \mathbb{C}[X] \quad P(X) &= \underbrace{\prod_{1 \leq i \leq p} (X - a_i)^{2\alpha_i}}_{T^2} \prod_{1 \leq j \leq q} (X - b_j)(X - \bar{b}_j) \\ &= T^2 \quad \text{où } T = \prod_{1 \leq i \leq p} (X - a_i)^{\alpha_i} \end{aligned}$$

$$P(X) = T^2 S \bar{S} = (TS)(\bar{T}\bar{S}) = Q \cdot \bar{Q} \quad \text{où } S = \prod_{1 \leq j \leq q} (X - b_j)$$

$$Q = A + iB \quad \text{où } A, B \in \mathbb{R}[X] \quad (\text{lemme facile})$$

$$\text{d'où } P(X) = (A + iB)(A - iB) = A^2 + B^2 \quad \text{où } A, B \in \mathbb{R}[X]$$

CQFD

⑨  $A(X) = X^3 - X - 1 \in \mathbb{R}[X]$

Racines réelles ?

$f(x) = x^3 - x - 1$

$x$	$-\infty$	$-\frac{1}{\sqrt{3}}$	$\frac{1}{\sqrt{3}}$	$+\infty$
$f'(x)$		+	0	-
$f(x)$	$\nearrow$	$\alpha$	$\searrow$	$\beta$

$\alpha = -\frac{1}{3^{\frac{3}{2}}} + \frac{1}{\sqrt{3}} - 1 \gtrless 0$

Il n'existe qu'une seule racine réelle

$\omega$ , et  $\omega > \frac{1}{\sqrt{3}}$ .

$\omega \notin \mathbb{Q}$

Si  $\omega = \frac{p}{q}$  où  $p, q \in \mathbb{Z}$   $\Delta(p, q) = 1$

Alors  $\omega^3 - \omega - 1 = 0 \Leftrightarrow p^3 - pq^2 - q^3 = 0 \Leftrightarrow p(p^2 - q^2) = q^3$

donc  $p \mid q^3 \Rightarrow$  (Th. Gauss)  $p \mid q$  car  $\Delta(p, q) = 1$ .

~~C'est absurde car alors  $\Delta(p, q) = p$ .~~

Mais  $p \mid q \Rightarrow \Delta(p, q) = |p| = 1$

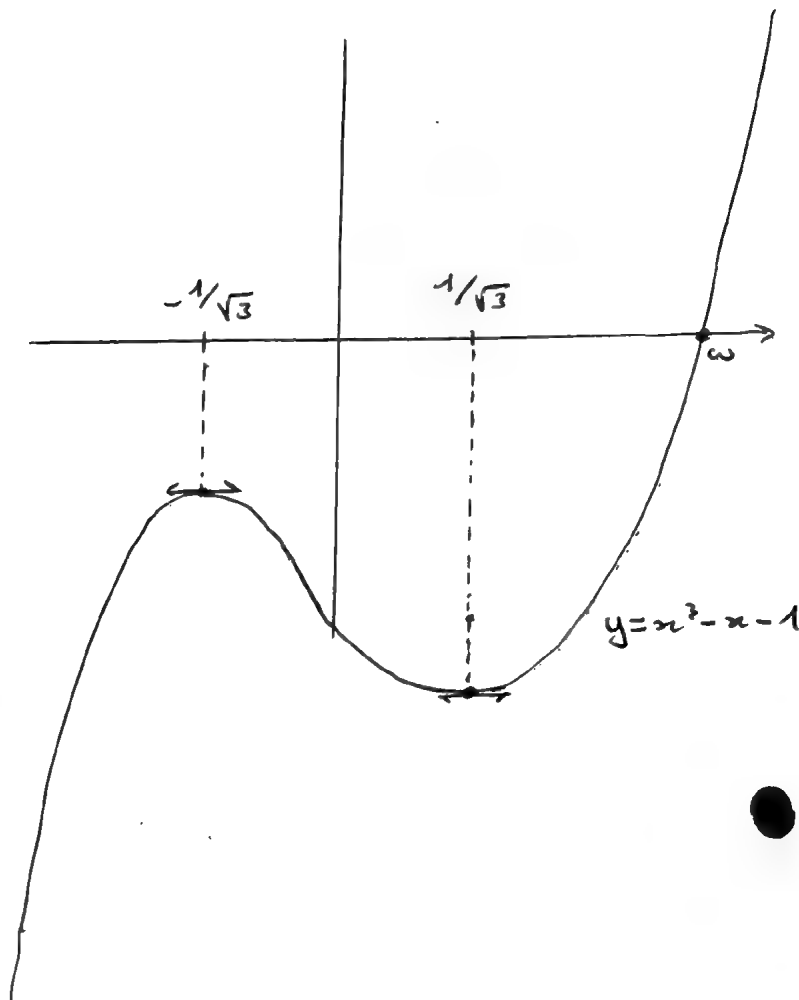
d'où  $\omega = \frac{1}{q}$  et  $1 - q^2 - q^3 = 0 \Rightarrow q^2(1 + q) = 1$

$\Rightarrow q \mid 1 \Rightarrow q = \pm 1 \Rightarrow \omega = \pm 1$ .

Il suffit de voir que  $\omega \neq \pm 1$ .

donc  $\omega \notin \mathbb{Q}$ .

$\mathbb{C} \setminus \mathbb{R}$





$\{1, \omega, \omega^2\}$  partie libre de  $\mathbb{Q}$ -ev  $\mathbb{R}$ .

$$\alpha, \beta, \gamma \in \mathbb{Q} \quad / \quad \alpha + \beta\omega + \gamma\omega^2 = 0 \quad (I)$$

Supposons que  $\gamma \neq 0$ .

$$\text{Alors } \omega^2 = -\frac{1}{\gamma}(\alpha + \beta\omega)$$

et, en reportant dans (II):  $\omega^3 - \omega - 1 = 0$ , on trouve:

$$-\frac{1}{\gamma}(\alpha\omega + \beta\omega^2) - \omega - 1 = 0$$

$\Updownarrow$

$$\bullet \quad -\frac{1}{\gamma}(\alpha\omega - \frac{\beta}{\gamma}(\alpha + \beta\omega)) - \omega - 1 = 0$$

$\Updownarrow$

$$\left(-1 - \frac{\alpha}{\gamma} + \frac{\beta^2}{\gamma^2}\right)\omega + \frac{\alpha\beta}{\gamma^2} - 1 = 0 \quad (1)$$

$$\ast \text{ Si } \left(-1 - \frac{\alpha}{\gamma} + \frac{\beta^2}{\gamma^2}\right) = 0, \text{ alors } \alpha\beta = \gamma^2.$$

Ainsi:  $\left\{ \begin{array}{l} \alpha\beta = \gamma^2 \Rightarrow \alpha\beta \neq 0 \\ \frac{\beta}{\gamma} = 1 + \frac{\alpha}{\gamma} \Rightarrow \left(\frac{\beta}{\alpha} - 1\right)^2 = \frac{\alpha^2}{\gamma^2} \Rightarrow \left(\frac{\beta}{\alpha} - 1\right)^2 = \frac{\alpha}{\beta} \end{array} \right.$

$$\bullet \quad \text{On a } t = \frac{\alpha}{\beta} \in \mathbb{Q}$$

On peut prendre  $\alpha = 1$

$$\left\{ \begin{array}{l} \gamma^2 = \beta \\ \beta^2 = \gamma^2 + \gamma \end{array} \right. \Rightarrow \left\{ \begin{array}{l} \gamma^4 = \gamma^2 + \gamma \\ \gamma^3 - \gamma - 1 = 0 \end{array} \right.$$

$$\text{Alors } \left(\frac{1}{t} - 1\right)^2 = t \Leftrightarrow \frac{1}{t^2} - \frac{2}{t} + 1 = t \Leftrightarrow t^3 - 2t^2 + t - 1 = 0 \Leftrightarrow t = \frac{-1 + \sqrt{5}}{2} \notin \mathbb{Q}, \text{ absurde.}$$

Donc:

cf. Autre solution: voir m TD p. 8

$$\ast \quad -1 - \frac{\alpha}{\gamma} + \frac{\beta^2}{\gamma^2} \neq 0. \text{ Mais alors (1)} \Rightarrow \omega \in \mathbb{Q}, \text{ absurde.}$$

Donc:

$$\underline{\underline{\gamma = 0}}$$

$$(I) \text{ devient } \alpha + \beta\omega = 0, \quad \left\{ \begin{array}{l} \beta \neq 0 \Rightarrow \omega = -\frac{\alpha}{\beta} \in \mathbb{Q}. \text{ Absurde} \\ \text{donc } \beta = 0 \Rightarrow \alpha = 0. \end{array} \right.$$

cqfd

⑥  $x = \frac{p}{q}$  où  $\Delta(p, q) = 1$

$$a \frac{p^2}{q^2} + b \frac{p}{q} + c = 0$$

$$ap^2 + bpq + cq^2 = 0 \quad (I)$$

Alors  $(ap + bq)p = -cq^2$   $c \neq 0 \Rightarrow q | ap + bq \Rightarrow q | ap \Rightarrow q | a$

Donc  $a = \lambda q$  (Gauss).

De la même façon, on montre que  $c = \mu p$ .

\* Si  $p$  ou  $q$  pair, alors  $a$  ou  $c$  pair et c'est terminé.

\* Supposons donc que  $p$  et  $q$  sont impairs. Alors (I) permet de conclure. En effet:  $p^2$  impair  $pq$  impair et  $q^2$  impair.

Si  $a, b$ , et  $c$  impairs, alors  $ap^2 + bpq + cq^2$  impair, absurde.

Donc  $a$ , ou  $b$ , ou  $c$  pair.

CQFD

⑦  $a, b, c, d \in \mathbb{Z}$

$$a^3 + b^3 + c^3 \equiv 0 \pmod{7} \Rightarrow abc \equiv 0 \pmod{7}$$

On constate que

$$a \not\equiv 0 \Rightarrow a^3 \equiv \pm 1.$$

et que:

$$a \not\equiv 0 \quad b \not\equiv 0 \quad \text{et} \quad c \not\equiv 0 \Rightarrow a^3 + b^3 + c^3 \not\equiv 0.$$

Donc  $a \equiv 0$  ou  $b \equiv 0$  ou  $c \equiv 0$

(Z/7Z)							
a	0	1	2	3	-3	-2	-1
a <sup>2</sup>	0	1	-3	2	2	-3	1
a <sup>3</sup>	0	1	1	-1	1	-1	-1

Le tableau nous donne aussi:  $a=1 \quad b=2 \quad c=3 \quad d=-2$

$$a^3 + b^3 + c^3 + d^3 \equiv 0 \text{ et pourtant } abcd = -12 \equiv 2 \pmod{7}$$

Gn a: (1) et (2)  $\Leftrightarrow$  (3)  $\Rightarrow$  (4)

$$\Downarrow$$

$$(4) \text{ et } uv = -\frac{p}{3}$$

Prendons  $p, q \in \mathbb{R}$  pour simplifier.

$$T^2 + qT - \frac{p^3}{27} = 0$$

$$\Delta = q^2 + \frac{4p^3}{27} = \frac{27q^2 + 4p^3}{27} \quad \text{s'appelle le "discriminant" de (1).}$$

C'est une définition bizarre, n'est-ce pas?

$$\Delta_{(1)} = 4p^3 + 27q^2$$

1) Si  $\Delta > 0$

Alors  $\exists U$  et  $V \in \mathbb{R}$  avec  $U = u^3$  et  $V = v^3$  où  $u, v \in \mathbb{R}$

Toutes les racines cubiques de  $U$  sont  $\{u, ju, j^2u\}$

" " "  $V$  sont  $\{v, jv, j^2v\}$

$$\text{Gn a } u^3v^3 = -\frac{p^3}{27} \Rightarrow uv = -\frac{p}{3} \quad \text{car } u \text{ et } v \text{ et } p \text{ réels.}$$

$$\text{Gn a: } \sqrt[3]{U} \quad \sqrt[3]{V}$$

$$\begin{array}{ccc} u & & v \\ ju & & jv \\ j^2u & & j^2v \end{array}$$

$$\text{Les solutions sont donc } x = \begin{cases} u+v \\ ju+j^2v \\ j^2u+jv \end{cases} \quad (\text{car on a aussi la condition } uv = -\frac{p}{3} \in \mathbb{R})$$

$$u^3 \neq v^3$$

$$\Downarrow$$

$$\text{Si } u \neq v \Rightarrow x = \begin{cases} u+v \\ ju+j^2v \notin \mathbb{R} \\ j^2u+jv \notin \mathbb{R} \end{cases}$$

Donc, si  $\Delta > 0$ , (1) n'admet qu'une racine réelle et a 2 racines conjuguées.

$$* P = X^n + \lambda_1 X^{n-1} + \dots + \lambda_n \quad \text{au} \quad P \in K[X] = I. \text{ Donc:}$$

$$P(\omega) = 0 = \omega^n + \lambda_1 \omega^{n-1} + \dots \Rightarrow \omega^n \in \text{ev engendré par } (1, \omega, \dots, \omega^{n-1})$$

$$\text{Donc } \omega^{n+1} \in \text{ev engendré } (1, \dots, \omega^{n-1})$$

2-démonstration:

$$\Phi: K[X] \rightarrow K$$

$$f \mapsto f(\omega)$$

$\Phi$  est une application  $K$ -linéaire de ces deux  $K$ -espaces vectoriels.

Et  $\text{Im } \Phi =$  ensemble des coefficients combinaisons linéaires à coefficients dans  $K$ , de toutes les puissances de  $\omega$ .

On a la décomposition canonique:

$$\begin{array}{ccc} K[X] & \xrightarrow{\Phi} & K \\ \downarrow & \nearrow & \uparrow \\ K[X] / \underbrace{\text{Ker } \Phi}_{\sim} & \xrightarrow{\sim} & \text{Im } \Phi \end{array}$$

$$\text{et } \dim \underbrace{K[X] / \text{Ker } \Phi}_I = \dim \underbrace{K[X] / P \in K[X]}_{P \in K[X]} = \deg P$$

$$\text{Donc } \boxed{\dim(\text{Im } \Phi) = \deg P.}$$

Retournons à l'exo 4:

$$\mathbb{Q}, \mathbb{R}$$

$$\begin{cases} A = X^3 - X - 1 \\ A(\omega) = 0 \end{cases}$$

$$\text{Soit } I = \{ f \in \mathbb{Q}[X] / f(\omega) = 0 \}$$

$$\text{On a déjà } A \in I$$

$$I = P \cdot \mathbb{Q}[X] \text{ où } P \in \mathbb{Q}[X]$$

$$\text{Donc } A \in I \Rightarrow A = PQ$$

Si  $\deg P \neq 3$ , alors  $\deg P$  ou  $\deg Q = 1$  et donc  $P$  ou  $Q$  possède une racine rationnelle, donc  $A$  aussi, ce qui est absurde.

$$\text{Donc } \deg P = 0 \text{ ou } \deg P = 3.$$

Si  $\deg P = 0$ ,  $P = 0$  (car  $P(\omega) = 0$ ), alors  $A = 0$  ce qui est faux car  $A = X^3 - X - 1$

$$\text{Donc } \deg P = 3, \quad P = \text{cte } A$$

$$A = \text{cte } P \Rightarrow I = A \cdot \mathbb{Q}[X]$$

$$(5) E_n = \{f \in \mathbb{R}[X] / \deg f \leq n\}$$

$$T: E_n \rightarrow E_n$$

$$f \mapsto T(f) = g \text{ où } g(X) = f(X+1) - f(X)$$

$$\dim E_n = n+1$$

\* Test linéaire

$$\text{On peut écrire } f(X+1) = f \circ L(X) \text{ où } L(X) = X+1$$

$$\text{où } \begin{cases} f = \sum_{i=0}^n a_i X^i \\ f \circ L = \sum_{i=0}^n a_i L^i \end{cases}$$

Remarque:  $f \in \mathbb{R}[X]$

$$A \xrightarrow{f_*} A \quad (A \text{ algèbre})$$

$$f \mapsto \sum_{i=0}^{\infty} a_i \delta^i$$

$$\text{* Si } \deg P = n, n \neq 0, \text{ alors } \deg T(P) = n-1$$

$$1 \xrightarrow{T} 0$$

$$X \xrightarrow{T} 1$$

$$X^2 \xrightarrow{T} 2X + 1$$

$\vdots$

$$X^n \xrightarrow{T} T(X^n) = (X+1)^n - X^n = nX^{n-1} + \dots$$

Ainsi,  $\forall k \in [1, n] \quad \deg(T(X^k)) = k-1$

Soit  $P \in E_n$ ,  $P = \sum_{i=0}^n a_i X^i \Rightarrow T(P) = \underbrace{a_n T(X^n)}_{\neq 0} + \dots + \underbrace{a_1 T(X)}_{\text{de degré} \leq n-1} + 0$

Noyau de T ?

$$P \in E_n / P(X+1) = P(X)$$

$$P \neq 0 \in \mathbb{R}[X] \Rightarrow \exists \alpha \in \mathbb{C} \quad P(\alpha) = 0$$

Mais alors  $\forall n \in \mathbb{N} \quad P(\alpha+n) = 0 \Rightarrow P$  admet une infinité de

racines ( $\mathbb{R} = \text{anneau com. intègre infini} \Rightarrow P=0$ )

donc  $\text{Ker } T = \{0\} \simeq \mathbb{R}$

Im T ?

$$E_n / E_0 \simeq \text{Im } T$$

$\Downarrow$

$$\left. \begin{array}{l} \dim \text{Im } T = n \\ \text{Mais } \text{Im } T \subset E_{n-1} \end{array} \right\} \Rightarrow \text{Im } T = E_{n-1}$$

## Application . (cf. Godement)

$$S_{n,m} = \sum_{1 \leq n \leq n} x^m$$

$$\exists f \mid \deg f = m+1 \quad f(x+1) - f(x) = x^m$$

Alors

$$\begin{cases} 1^m = f(2) - f(1) \\ 2^m = f(3) - f(2) \\ \dots \\ n^m = f(n+1) - f(n) \end{cases}$$

$$S_{n,m} = f(n+1) - f(1)$$

Si  $m=2$ , on calcule facilement  $\sum_{n=1}^n x^2$

$$f(x) = ax^3 + bx^2 + cx \Rightarrow T(f) = a[(x+1)^3 - x^3] + b[(x+1)^2 - x^2] + c[x+1 - x]$$

$$T(f) = a(3x^2 + 3x + 1) + b(2x + 1) + c = x^2$$

$$a = \frac{1}{3} \text{ donc } x^2 + x + \frac{1}{3} + b(2x+1) + c = x^2$$

$$b = -\frac{1}{2}$$

$$\frac{1}{3} - \frac{1}{2} + c = 0 \Rightarrow c = \frac{1}{6}$$

donc

$$f(x) = \frac{1}{3}x^3 - \frac{1}{2}x^2 + \frac{1}{6}x$$

$$\text{Donc } \sum_{n=1}^n x^2 = \frac{1}{3}(n+1)^3 - \frac{1}{2}(n+1)^2 + \frac{1}{6}(n+1) - 0$$

$$\sum_{n=1}^n x^2 = \frac{n(n+1)(2n+1)}{6}$$

Remarques: 1)

$$p_k = \frac{x(x-1) \dots (x-k+1)}{k!} = \in$$

$$T(p_k) = \frac{(x+1)x(x-1) \dots (x-k+2) - x(x-1) \dots (x-k+1)}{k!}$$

$$= \frac{x(x-1) \dots (x-k+2) [\cancel{x+1} - \cancel{x+k-1}]}{k!}$$

$$= p_{k-1}$$

(cf.  $C_n^k$ )

$$2) \begin{cases} T^k(p) = T(T^{k-1}p) \\ T^0 p = p \end{cases}$$

$$p = \sum_{k=0}^{\infty} (T^k p)(0) p_k$$

⑧ (Grand théorème de Fermat:  $x^n + y^n = z^n$  n'a pas de solutions pour  $n \geq 3$ )

$$\boxed{x^2 + y^2 = z^2} \quad (1) \quad \text{dans } \mathbb{N} \quad (\text{puisque après, c'est facile, dans } \mathbb{Z})$$

$$\text{Soit } d = \Delta(x, y, z) \quad \begin{cases} x = d x' \\ y = d y' \\ z = d z' \end{cases}$$

$$\text{D'après (1)} \Rightarrow x'^2 + y'^2 = z'^2 \text{ où } \Delta(x', y', z') = 1$$

$$\text{Résoudre (1) équivaut à résoudre (2): } \begin{cases} x^2 + y^2 = z^2 \\ \Delta(x, y, z) = 1. \end{cases}$$



Pro Si  $x^2 + y^2 = z^2$  et  $\delta(x, y, z) = 1$ , alors  $x, y, z$  sont premiers entre eux deux à deux.

$$\text{Si } \delta | x \text{ et } y \Rightarrow \delta^2 | z^2 \Rightarrow \delta | z \Rightarrow \delta = \pm 1$$

Si  $z$  pair, alors  $z^2$  est divisible par 4. Mais  $x$  et  $y$  impairs, donc  $x^2 + y^2 = 4u + 2$  d'où  $x^2 + y^2 \equiv 2 \pmod{4}$  et  $z^2 \equiv 0 \pmod{4}$ , donc  $z$  pair ne peut être solution.

Donc, forcément  $z$  est impair.

Donc  $x$  et  $y$  ont des parités différentes. Supposons que  $x$  soit impair et  $y$  pair (Symétrie entre  $x$  et  $y$ )

1<sup>re</sup> méthode : Solution algébrique.

$$y^2 = z^2 - x^2 = (z-x)(z+x)$$

$$\delta = \delta(z-x, z+x) \Rightarrow \delta \mid \begin{matrix} 2z \\ 2x \end{matrix}$$

$$\text{Comme } z-x \text{ et } z+x \text{ pair, } \delta = 2\delta' \Rightarrow \delta' \mid \begin{matrix} x \\ z \end{matrix} \Rightarrow \delta' = 1 \quad \text{car } \delta(x, z) = 1$$

$$\text{Donc } \delta(z-x, z+x) = 2$$

On écrit :

$$\frac{y^2}{4} = \frac{z-x}{2} \cdot \frac{z+x}{2} \quad \text{et} \quad \delta\left(\frac{z-x}{2}, \frac{z+x}{2}\right) = 1$$

$$\left(\frac{y}{2}\right)^2$$

lemme

$$\boxed{\begin{array}{l} a^2 = uv \quad \delta(u, v) = 1 \\ \text{Alors } \exists \alpha, \beta \quad u = \alpha^2 \quad v = \beta^2 \end{array}}$$

$$\text{Preuve } \delta = \delta(a, u) \quad a = \delta a' \quad u = \delta u' \quad \delta(a', u') = 1$$

$$\delta^2 a'^2 = \delta u' v \Rightarrow \delta a'^2 = u' v \Rightarrow u' \mid \delta a'^2 \Rightarrow \exists u' \mid \delta \quad \text{on note } \delta = u' \delta' \quad (\text{Gauss})$$

$$\text{d'où } \delta' \nmid \alpha'^2 = \alpha' \nu \Rightarrow \delta' \mid \nu$$

$$\text{or } \delta' \mid \delta \mid u \Rightarrow \delta' \mid u \Rightarrow \left. \begin{matrix} \delta' \mid u \\ \delta' \mid \nu \end{matrix} \right\} \Rightarrow \delta' = 1$$

$$\text{d'où } \alpha'^2 = \nu$$

$$\text{et } \delta = u' \text{ et } u = u'^2$$

QED

(NB: 2-dém. avec les valuations)

$$\text{Par application de ce lemme : } \exists \alpha, \beta \quad \begin{cases} \frac{z-x}{2} = \alpha^2 \\ \frac{z+x}{2} = \beta^2 \end{cases}$$

$$\begin{cases} z-x = 2\alpha^2 \\ z+x = 2\beta^2 \end{cases} \Rightarrow \begin{cases} z = \alpha^2 + \beta^2 \\ x = \beta^2 - \alpha^2 \end{cases}$$

$$\text{d'où } y^2 = z^2 - x^2 = 2\alpha\beta$$

$$\begin{cases} x = \beta^2 - \alpha^2 \\ y = 2\alpha\beta \\ z = \alpha^2 + \beta^2 \end{cases} \quad \delta(\alpha, \beta) = 1 \text{ et } \alpha \neq \beta \quad \{2\} \text{ car } x \text{ impair.}$$

$$\begin{aligned} & \updownarrow \\ & \boxed{\begin{aligned} x^2 + y^2 &= z^2 \quad (x \text{ impair, } y \text{ pair}) \\ \delta(x, y, z) &= 1 \end{aligned}} \end{aligned}$$

$$\Downarrow \quad * \begin{cases} x^2 + y^2 = \beta^4 + \alpha^4 \pm 2\alpha^2\beta^2 + 4\alpha^2\beta^2 = (\alpha^2 + \beta^2)^2 = z^2 \\ z^2 = (\alpha^2 + \beta^2)^2 \end{cases} \text{ oui.}$$

$$* \begin{cases} x \text{ impair} \\ y \text{ pair} \end{cases} \text{ évident.}$$

$$* \text{ Enfin } \delta(x, y, z) = 1 \text{ puisque, si } d \text{ est un diviseur commun à } \beta^2 - \alpha^2$$

$$2\alpha\beta \text{ et } \alpha^2 + \beta^2$$

$$\text{Alors } d \mid 2\beta^2 \quad d \mid 2\alpha^2 \text{ et } d \mid 2\alpha\beta.$$

$$d \text{ n'est pas pair car } d \mid \underbrace{\beta^2 - \alpha^2}_{\text{impair}}. \text{ Donc } \delta(d, 2) = 1 \Rightarrow \begin{cases} d \mid \alpha^2 \\ d \mid \beta^2 \end{cases} \text{ et } d \mid \alpha\beta$$

$\Downarrow$

$$d = 1$$

$$(\text{car } \delta(\alpha^2, \beta^2) = 1)$$

● Solutions classiques :  $\begin{cases} x = 3 \\ y = 4 \\ z = 5 \end{cases}$

y-a-t'il plus de solutions consécutives?

$$n^2 + (n+1)^2 = (n+2)^2$$

$$n^2 - 2n - 3 = 0$$

$$\Delta' = 1 + 3 = 4$$

$$1 \pm 2 \mid \begin{matrix} 3 \\ -1 \end{matrix}$$

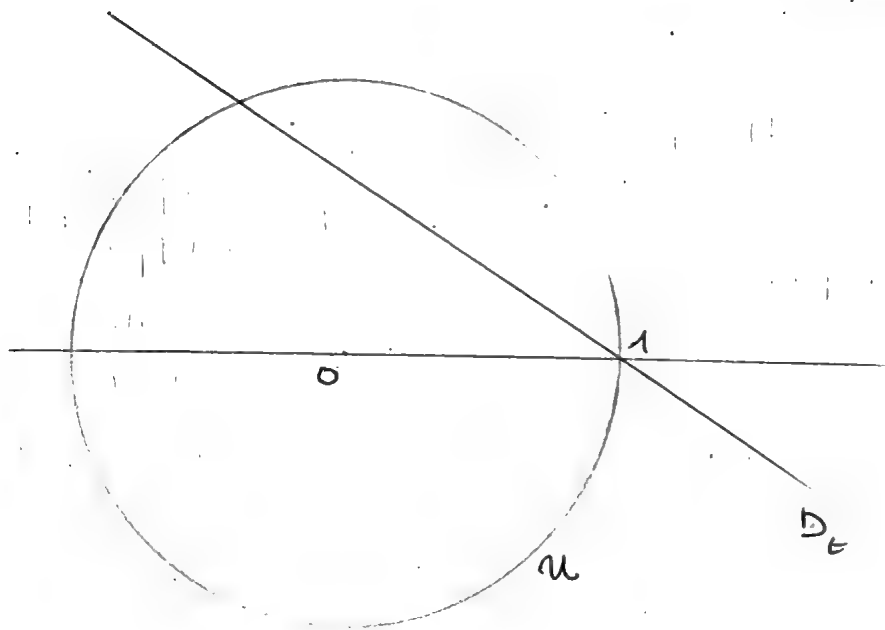
●  $(n+1)(n-3) = 0 \Rightarrow \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \\ +1 \end{pmatrix} \text{ ou } \begin{pmatrix} 3 \\ 4 \\ 5 \end{pmatrix}$

2<sup>e</sup> méthode : Solution géométrique.

$$\left(\frac{x}{3}\right)^2 + \left(\frac{y}{4}\right)^2 = 1$$

$$X^2 + Y^2 = 1$$

Problème : trouver les pts à coordonnées rationnelles sur le cercle unité  $\mathcal{U}$ .



$\begin{cases} x=1 \\ y=0 \end{cases}$  solution.

$$Y = t(1-X)$$

Cherchons  $D_t \cap U$  :

$$t^2(1-X)^2 = (1-X)^2$$

$\Downarrow$

$$t^2(1-X) = 1+X \quad (t \neq 1)$$

$\Downarrow$

$$X(1+t^2) = t^2 - 1$$

$\Downarrow$

$$\begin{cases} X = \frac{t^2 - 1}{t^2 + 1} = \frac{x}{y} \\ Y = \frac{2t}{t^2 + 1} = \frac{z}{y} \end{cases}$$

Ainsi, si  $t \in \mathbb{Q}$   $t = \frac{p}{q}$   $\Delta(p, q) = 1$

$$\text{et } \begin{cases} x = \frac{p^2 - q^2}{p^2 + q^2} z \\ y = \frac{2pq}{p^2 + q^2} z \end{cases}$$

Enchâssé, rappelons le,  $\begin{pmatrix} x \text{ impair} \\ y \text{ pair} \\ \Delta(x, y, z) = 1 \end{pmatrix}$

$d = \Delta(p^2 + q^2, p^2 - q^2)$ , alors  $d \mid p^2$  et  $d \mid q^2 \Rightarrow d = 1$  ou  $2$ .

(si d impair...  
si d pair...)

$$\textcircled{1} d = 1 \Rightarrow p^2 + q^2 \mid (p^2 - q^2)z \Rightarrow \begin{cases} z = \lambda(p^2 + q^2) \\ x = \lambda(p^2 - q^2) \\ y = 2\lambda pq \end{cases} \Rightarrow \lambda = 1 \Rightarrow \begin{cases} z = p^2 + q^2 \\ x = p^2 - q^2 \\ y = 2pq \end{cases}$$

②  $d=2 \Rightarrow p \text{ et } q \text{ impairs} \Rightarrow x \text{ est pair (car } p^2 - q^2 \equiv 0[4])$

donc  $x$  divisible par 4

Or  $p^2 + q^2$  est divisible par 2, mais pas plus.

Donc  $x$  pair, c'est absurde.

Remarque:

$\mathbb{Z}[i] = \{a+ib / a, b \in \mathbb{Z}\}$  est un anneau euclidien.

$\mathbb{Z}[i\sqrt{5}]$  n'est pas principal.

A prouver:  $x^4 + y^4 = z^2$  non résoluble avec  $x, y, z > 0$

$\Downarrow$

non plus  $x^4 + y^4 = z^4$ .

Preuve: Soit  $d = \Delta(x, y, z)$

$$\begin{cases} x = d x' \\ y = d y' \\ z = d z' \end{cases}$$

$$d^4(x'^4 + y'^4) = d^2 z'^2$$

$$d^2(x'^4 + y'^4) = z'^2$$

$$\text{donc } d^2 | z'^2 \Rightarrow d | z' \Rightarrow z' = d z''$$

$$x'^4 + y'^4$$

Lemme:  $d^2 | z'^2 \Rightarrow \cancel{z} d | z'$

Preuve:  $\delta = \Delta(d, z')$

$$\begin{cases} d = \delta d' \\ z' = \delta z'' \end{cases} \Rightarrow \cancel{\delta}^2$$

D'où  $\delta^2 z''^2 = \delta^2 d'^2 \Rightarrow z''^2 = \delta^2 d'^2$

$$\left. \begin{array}{l} \Delta(d', z'') = 1 \\ \Rightarrow d' | z'' \text{ (lemme de Gauss)} \\ \Rightarrow d' = 1 \end{array} \right\}$$

donc  $d|z'$

d'où  $x'^4 + y'^4 = z''^2$  où  $\Delta(x', y', z'') = 1$

premiers dans leur ensemble.

$$\begin{cases} x'^2 = \alpha^2 - \beta^2 \\ y'^2 = 2\alpha\beta \\ z'' = \alpha^2 + \beta^2 \end{cases} \Rightarrow x'^2 + \beta^2 = \alpha^2 \Leftrightarrow$$

et  $\Delta(x', \alpha, \beta) = 1$

où  $\Delta(\alpha, \beta) = 1$

$$\begin{cases} x' = u^2 - v^2 \\ \beta = 2uv \text{ (forcément pair)} \\ \alpha = u^2 + v^2 \end{cases}$$

où  $\Delta(u, v) = 1$

Donc  $y'^2 = 4\alpha uv \Rightarrow \alpha uv$  est un carré

$\Downarrow$   $\alpha, u$  et  $v$  sont premiers entre eux deux à deux  
(Si  $p \in \mathbb{P}$   $p|\alpha$  et  $u$ , alors  $p|v^2 \Rightarrow p|v \Rightarrow p=1$ .  
Donc  $\exists p \in \mathbb{P} : p|\alpha$  et  $u$   
 $\Downarrow$   
 $1 = \Delta(\alpha, u)$ )  
 $\alpha, u$  et  $v$  sont des carrés.

On peut écrire  $\begin{cases} \alpha = A^2 \\ u = U^2 \\ v = V^2 \end{cases}$

d'où

$$A^2 = U^4 + V^4$$

on avait  $\Delta(u, v) = 1 \Rightarrow \Delta(U, V) = 1$

donc  $\Delta(A, U, V) = 1$ .

Je prétends que les solutions de cette équation sont plus petites que les solutions précédentes :

On a  $\boxed{0 < A < z'}$  puisque  $A = \sqrt{\alpha} \leq \alpha \leq \underbrace{\alpha^2}_{< z} < z$   
car  $z = \alpha^2 + \beta^2$

On suppose  $\exists \text{ sol } x^4 + y^4 = z^2 \quad (>0)$

$$z_1 = \inf \{ z > 0 / \exists x, y / x^4 + y^4 = z^2 \} > 0$$

Mais on sait fabriquer une solution  $A$  plus petite, ce qui contredit  $z_1 = \inf \{ \}$ . Donc  $\exists$  solution  $x^4 + y^4 = z^2$ . (QFD)

(Procédée de descente infinie de Fermat)

(11)  $G = \text{groupe commutatif d'ordre } n \Rightarrow G \text{ cyclique}$   
 où  $n = \prod_{i=1}^I p_i$

$n = \prod_{i=1}^I p_i$   $G$  est un gartf et donc  $G \simeq \prod_{j=1}^k \mathbb{Z}/d_j\mathbb{Z}$  où  $d_j | d_{j+1}$

On a  $d_1 \dots d_k = n$  (1)

(1)  $\Rightarrow d_1 | n \Rightarrow d_1 = \prod_{i=1}^I p_i^{\alpha_i^1}$  où  $\alpha_i^1 = 1 \text{ ou } 0$

$d_1 | d_2 | n \Rightarrow d_2 = \prod_{i=1}^I p_i^{\alpha_i^2}$  où  $\alpha_i^2 = 1 \text{ ou } 0$  et  $\alpha_i^2 \geq \alpha_i^1$

-----

$d_1 | \dots | d_k | n \Rightarrow d_k = \prod_{i=1}^I p_i^{\alpha_i^k}$  où  $\alpha_i^k \geq \alpha_i^{k-1} \geq \dots \geq \alpha_i^1$

De plus, (1)  $\Rightarrow \sum_{j=1}^k \alpha_i^j = 1 \quad (\forall i) \quad (2)$

Si  $\exists i \in [1, I] / \exists j \in [1, k[ \quad \alpha_i^j = 1$

alors  $\alpha_i^k \geq \alpha_i^{k-1} \geq \dots \geq \alpha_i^j = 1 \Rightarrow \alpha_i^k = \dots = \alpha_i^j = 1$

donc  $\sum_{j=1}^k \alpha_i^j \geq 2$ , impossible

Donc :  $\forall i \in [1, I] \quad \forall j \in [1, k[ \quad \alpha_i^j = 0$

$\Downarrow$

$$\begin{cases} d_1 = \dots = d_{k-1} = 1 \\ \text{et } d_k = \prod_{i=1}^I p_i = n \end{cases}$$

D'où  $G \simeq \mathbb{Z}/\mathbb{Z} \times \dots \times \mathbb{Z}/\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n\mathbb{Z}$

CQFD



$$\begin{cases} v(e_1) = 0 \\ v(e_2) = e_3 \\ v(e_3) = e_4 = v^2(e_2) \\ v(e_4) = 0 \end{cases}$$

$$v^3 = 0$$

$$\text{Ker } v \subset \text{Ker } v^2 \subset \text{Ker } v^3 = E$$

$\neq$

$\neq$

$$\text{car } (x-1)^2 \times \left[ \frac{k[x]}{(x-1)} \times \frac{k[x]}{(x-1)^2} \right] \neq 0 \quad \forall x.$$

$$(\text{car } \text{Ker } v = \text{Ker } v^2 \Rightarrow \text{Ker } v^2 = \text{Ker } v^3.)$$

~~Si l'on a~~

$$\left. \begin{array}{l} \text{On sait que } \dim \text{Ker } v = 2 \\ \dim \text{Ker } v^3 = 4 \end{array} \right\} \Rightarrow 2 < \dim \text{Ker } v^2 < \dim E \Rightarrow \dim \text{Ker } v^2 = 3.$$

Prendons

$$\begin{cases} e_2 \notin \text{Ker } v^2 \\ e_2 \neq 0 \\ e_3 = v(e_2) \\ e_4 = v(e_3) \end{cases}$$

~~Cette base~~

Ce système  $(e_1, e_2, e_3, e_4)$  est libre car  $\lambda_2 e_2 + \lambda_3 e_3 + \lambda_4 e_4 = 0$

$$\Downarrow$$

$$\lambda_2 = \lambda_3 = \lambda_4 = 0$$

On prend  $e_1 \in (\text{supplémentaire de } e_4 \text{ dans } \text{Ker } v).$

Alors  $(e_1, e_2, e_3, e_4) = \text{base}$  telle que

$$\begin{cases} v(e_1) = 0 \\ v(e_2) = e_3 \\ v(e_3) = e_4 \\ v(e_4) = 0 \end{cases}$$

$$d) \begin{pmatrix} 6 & 20 & -34 \\ 6 & 32 & -51 \\ 4 & 20 & -32 \end{pmatrix} = u \quad \begin{matrix} \text{est semblable à} \\ \text{et équivalente à} \end{matrix} \begin{pmatrix} x & & \\ & x-2 & \\ & & x-2 \end{pmatrix}$$

$$u \text{ est semblable à } w = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 1 & 2 \end{pmatrix}$$

$$E \simeq K[X] / (X-2)$$

$$\text{car } u - XI \text{ est équivalente à } \begin{pmatrix} 1 & 0 & 0 \\ 0 & X-2 & 0 \\ 0 & 0 & (X-2)^2 \end{pmatrix}$$

Base où cette matrice se met sous forme de Jordan.

$$\text{Posons } \begin{cases} v = u - 2I \\ v^2 = 0 \end{cases}$$

$$\text{Problème : Trouver } (e_1, e_2, e_3) \text{ tels que } \begin{cases} v(e_1) = 0 \\ v(e_2) = e_3 \\ v(e_3) = 0 \end{cases}$$

Trouver  $v(e_2) \neq 0$ ?

$e_2 \notin \text{Ker } v$ , si  $e_2(x, y, z)$  alors :

$$\begin{cases} 4x + 20y - 34z \neq 0 \\ 6x + 30y - 51z \neq 0 \\ 4x + 20y - 34z \neq 0 \end{cases}$$

$$\text{Prendons } \boxed{e_2 = (1, 0, 0)}$$

$$\text{Prendons } \boxed{e_3 = v(e_2) = \begin{pmatrix} 4 \\ 6 \\ 4 \end{pmatrix}}$$

$$\text{Noyau de } v : \begin{cases} 4x + 20y - 34z = 0 \\ 6x + 30y - 51z = 0 \end{cases} = (\text{Ker } v)$$

Prendons  $e_1$  dans  $\text{Ker } v$  et tel que  $(e_1, e_3)$  libre, par exemple

$$\boxed{e_1 = \begin{pmatrix} 5 \\ -1 \\ 0 \end{pmatrix}}$$

$$\underbrace{\otimes}_{\mathbb{Z} \times \mathbb{Z}} \cdot \begin{pmatrix} 0 & \dots & \alpha_1 \\ & \ddots & \\ & & 0 \\ \alpha_n & & & 0 \end{pmatrix} = u \quad (\text{dans } \mathbb{C})$$

$(e_i, e_{n-i+1})$  = o.e.v. stable.

$$\begin{cases} u(e_1) = \alpha_1 e_n \\ u(e_n) = \alpha_n e_1 \end{cases} \quad u(e_i) = \alpha_{n-i+1} e_{n-i+1}$$

Posons  $E_i = (e_i, e_{n-i+1})$

$$i = n-i+1 \Leftrightarrow 2i = n+1$$

Si  $n$  pair, ils sont tous de dimension 2  
 Si  $n$  impair, il existe un seul  $E_i$  (pour  $i = \frac{n+1}{2}$ ) de dimension 1, les autres étant de dim 2.

Si  $n$  pair  $E = \bigoplus_{1 \leq i \leq m} E_i \quad u(E_i) \subset E_i$

Dans  $E_i$ , la matrice est  $\begin{pmatrix} 0 & \alpha_i \\ \alpha_{n-i+1} & 0 \end{pmatrix}$ .

On appelle que :

$u$  diagonalisable  $\Leftrightarrow P_H$  a toutes ses racines simples.

$\Leftrightarrow P_H = \text{ppcm}(P_{H_1}, \dots, P_{H_k})$  a toutes ses racines simples.

~~$E = \bigoplus_{i=1}^k E_i$~~   
 $(P_i)$

Th  $E = \bigoplus E_i \quad u \in \text{Ind}(E) / u(E_i) \subset E_i$

$P_H$  = polynôme minimal de  $u$

$P_{H_i}$  = " " de  $u_i: E_i \rightarrow E_i$

Alors  $P_H = \text{ppcm}(P_{H_i})_{1 \leq i \leq m}$

$$E_i = \bigoplus_j \mathbb{K}[X] / (P_j^i) \quad \text{et} \quad \text{Ann}_{\mathbb{K}[X]} E_i = P_{H_i}$$

Donc  $E = \bigoplus N_i$   $N_i =$  sous- $\mathbb{K}[X]$ -modules  $\dots = E_i$   
 $\text{Ann } N_i = P_{H_i}$

oui: En effet:  $x = (x_1, \dots, x_m)$

$$\forall x \quad \lambda x = 0 \Leftrightarrow \begin{cases} \lambda x_i = 0 \\ \forall i \end{cases} \Leftrightarrow \forall i \exists P_{H_i} \mid \lambda \Leftrightarrow \lambda \text{ mult. de } \text{ppcm}(P_{H_i})$$

En particulier, le  $\text{ppcm}(P_{H_i})$  convient.

Donc  $\text{ppcm}(P_{H_i}) = P_H$

QFD

$$\begin{pmatrix} \alpha & \gamma \\ \beta & 0 \end{pmatrix} = H_i$$

\* Si  $\alpha = \beta = 0$   $P_{H_i} = 0$

\* Si  $\alpha$  ou  $\beta \neq 0$   $P_{H_i} = X^2 - \alpha\beta$

Montrons que

$$P_H \mid u \text{ diagonalisable} \Leftrightarrow u_i \text{ diagonalisable}$$

( $\Leftarrow$ ) trivial

( $\Rightarrow$ )  $u$  diagonalisable  $\Rightarrow P_H$  n'a que des rac. simples.

$\Rightarrow \forall i$   $P_{H_i}$  n'a que des racines simples.

$\Rightarrow u_i$  diagonalisable.

3.7.79

## Feuille N°7

× 1<sup>er</sup> Montrer que le pgcd des polynômes  $X^n - 1$  et  $X^m - 1$  est  $X^d - 1$  où  $d = \text{pgcd}(n, m)$ .

× 2<sup>er</sup> Trouvez des matrices diagonales équivalentes aux matrices suivantes (le corps de base est  $\mathbb{C}$ ).

$$\begin{pmatrix} X & 1 \\ 0 & X \end{pmatrix} \quad \begin{pmatrix} X^2 - 1 & X + 1 \\ X + 1 & X^2 + 2X + 1 \end{pmatrix} \quad \begin{pmatrix} 1 - X & X^2 & X \\ X & X & -X \\ 1 + X^2 & X^2 & -X^2 \end{pmatrix}$$

$$\bullet \begin{pmatrix} X & 1 & 0 & 0 \\ 0 & X & 1 & 0 \\ 0 & 0 & X & 1 \\ 0 & 0 & 0 & X \end{pmatrix} \quad \text{et c....}$$

× 3<sup>er</sup> Montrer que les matrices  $\begin{pmatrix} 3 & 2 & -5 \\ 2 & 6 & -10 \\ 1 & 2 & -3 \end{pmatrix}$  et

$\begin{pmatrix} 6 & 20 & -34 \\ 6 & 32 & -51 \\ 4 & 20 & -32 \end{pmatrix}$  sont semblables en calculant leurs invariants de similitude ; même question pour

$$\begin{pmatrix} 4 & 10 & -13 & 4 \\ 1 & 6 & -8 & 3 \\ 1 & 4 & -6 & 2 \\ 0 & -1 & 1 & 0 \end{pmatrix} \text{ et } \begin{pmatrix} 41 & -4 & -26 & -7 \\ 14 & -13 & -31 & -18 \\ 40 & -4 & -25 & -8 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

4° Mettre sous la forme de Jordan les matrices suivantes (on calcule dans chaque cas le changement de base permettant de se ramener à la forme de Jordan) :  $\begin{pmatrix} 0 & 1 & 0 \\ -4 & 4 & 0 \\ -2 & 1 & 2 \end{pmatrix}$ ,  $\begin{pmatrix} 12 & -6 & -2 \\ 18 & -3 & -3 \\ 18 & -3 & -3 \end{pmatrix}$ .

$$\begin{pmatrix} 1 & -3 & 0 & 3 \\ -2 & -6 & 0 & 13 \\ 0 & -3 & 1 & 3 \\ -1 & -4 & 0 & 8 \end{pmatrix} ; \begin{pmatrix} 0 & 0 & 0 & \dots & n \\ & & & & \\ & & & & \\ 0 & n & n-1 & \dots & 2 \\ n & n-1 & n-2 & \dots & 1 \end{pmatrix}$$

5° Montrer que si  $A = \begin{pmatrix} a & 1 & 0 & \dots & 0 \\ 0 & a & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a & 1 \\ 0 & 0 & \dots & 0 & a \end{pmatrix}$  est une

matrice de Jordan d'ordre  $n$  et si  $f(x)$  est un polynôme à une variable, alors

$$f(A) = \begin{pmatrix} f(a) & f_1(a) & f_2(a) & \dots & f_{n-1}(a) \\ 0 & f(a) & f_1(a) & \dots & f_{n-2}(a) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & f(a) & f_1(a) \\ 0 & 0 & \dots & 0 & f(a) \end{pmatrix}$$

où l'on pose  $f_k(a) = \frac{1}{k!} f^{(k)}(a)$ . Ceci suppose que le corps de base soit de caractéristique 0. Que se passe-t-il en caractéristique  $p \neq 0$ ?

$$\textcircled{2} \quad \begin{pmatrix} X & 1 \\ 0 & X \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 0 & X^2 \end{pmatrix}$$

$$\begin{pmatrix} X^2-1 & X+1 \\ X+1 & X^2+2X+1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} X+1 & 0 \\ 0 & P_2 \end{pmatrix} \quad (1)$$

$$\text{ou} \quad (X+1) P_2 = (X^2-1)(X^2+2X+1) - (X+1)^2$$

$$(X+1) P_2 = (X+1)^2 (X^2-2)$$

$$\bullet \text{ d'ou } P_2 = (X+1)(X^2-2)$$

$$\text{done} \quad (1) \rightsquigarrow \begin{pmatrix} X+1 & 0 \\ 0 & (X+1)(X^2-2) \end{pmatrix}$$

$$\begin{pmatrix} 1-X & X^2 & X \\ X & X & -X \\ 1+X^2 & X^2 & -X^2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & X^2 & X \\ 0 & X & -X \\ 1 & X^2 & -X^2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & X^2 & X \\ 0 & X & -X \\ 0 & 0 & -X^2-X \end{pmatrix}$$

$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & X & -X \\ 0 & 0 & -X^2-X \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & X & 0 \\ 0 & 0 & X^2+X \end{pmatrix}$$

$$\begin{pmatrix} X & 1 & 0 & 0 \\ 0 & X & 1 & 0 \\ 0 & 0 & X & 1 \\ 0 & 0 & 0 & X \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & X^2 & 1 & 0 \\ 0 & 0 & X & 1 \\ 0 & 0 & 0 & X \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & X^3 & 1 \\ 0 & 0 & 0 & X \end{pmatrix}$$

$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & X^4 \end{pmatrix}$$

Donner

$$\underbrace{\begin{pmatrix} X & 1 & 0 \\ & X & 1 & 0 \\ & & \ddots & \ddots & \ddots \\ 0 & & & 1 & X \end{pmatrix}}_{n \text{ colonnes}} \quad n \text{ lignes} \quad \sim \quad \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & X^n \end{pmatrix}$$

$$\textcircled{3} \quad \begin{pmatrix} 3 & 2 & -5 \\ 2 & 6 & -10 \\ 1 & 2 & -3 \end{pmatrix} = u \quad \begin{pmatrix} 6 & 20 & -34 \\ 6 & 32 & -51 \\ 4 & 20 & -32 \end{pmatrix} = v$$

$$u - XI = \begin{pmatrix} 3-X & 2 & -5 \\ 2 & 6-X & -10 \\ 1 & 2 & -3-X \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & X-2 & 0 \\ 0 & 0 & -X^2+4X-4 \end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & X-2 & 0 \\ 0 & 0 & (X-2)^2 \end{pmatrix}$$

$$\text{et} \quad v - XI = \begin{pmatrix} 6-X & 20 & -34 \\ 6 & 32-X & -51 \\ 4 & 20 & -32-X \end{pmatrix} \sim \begin{pmatrix} -X & -12+X & 17 \\ 6 & 32-X & -51 \\ 4 & 20 & -32-X \end{pmatrix} \quad \times \frac{1}{17}(X+1)$$

$$\sim \begin{pmatrix} 1 & -12+X & 17 \\ -3(X+1)+6 & 32-X & -51 \\ +4 & 20 & -32-X \end{pmatrix} = \begin{pmatrix} 1 & X-12 & 17 \\ -3X+3 & -X+32 & -51 \\ -\frac{1}{17}(X^2+33X+32) & 20 & -X-32 \end{pmatrix}$$

$$- \frac{1}{17}(X+1)(X+32)$$

$$\sim \begin{pmatrix} 1 & 0 & 0 & 17 \\ -3X+3 & 3X^2-40X+68 & -51 \\ -\frac{1}{17}(X^2+33X+32) & & \end{pmatrix}$$

trop dur. Prenons  
une autre méthode



Calculons tous les mineurs d'ordre 2.

On trouve :

$$P_1 P_2 = \text{pgcd} \left( (x-2)(x-36), 20(2-x), 4(x-2), 34(2-x), 20(2-x), \right. \\ \left. (x-2)(x+2), 51(x-2), (x-2)(x+28), 6(2-x) \right)$$

$$P_1 = 1, \text{ d'où } P_2 = x-2.$$

$$\text{Donc } \det(v - XI) = P_3(x-2) = -(x-2)^3 \Rightarrow P_3 = \pm (x-2)^3$$

d'où

$$v - XI \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & x-2 & 0 \\ 0 & 0 & (x-2)^2 \end{pmatrix}$$

Rappelons le théorème :

Th

$M$  = matrice à coefficients dans un corps  $k$ , et  $n \times n$ .

$$M \text{ et } N \text{ semblables} \Leftrightarrow \left\{ \begin{array}{l} M - XI \text{ et } N - XI \text{ ont même} \\ \text{diviseurs élémentaires} \\ \text{dans } K[X] \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} M - XI \\ \text{et } N - XI \\ \text{équivalentes} \end{array} \right\}$$

↓  
ces div. él. sont appelés  
"invariants de similitude".

④

$$u) \begin{pmatrix} 0 & 1 & 0 \\ -4 & 4 & 0 \\ -2 & 1 & 2 \end{pmatrix} = u$$

$$\begin{pmatrix} -x & 1 & 0 \\ -4 & 4-x & 0 \\ -2 & 1 & 2-x \end{pmatrix} \leadsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & x-2 & 0 \\ 0 & 0 & (x-2)^2 \end{pmatrix}$$

$$E \simeq K[X]/(X-2) \oplus K[X]/(X-2)^2$$

$$u \text{ semblable à } \left( \begin{array}{c|cc} 2 & 0 & 0 \\ \hline 0 & 2 & 0 \\ 0 & 1 & 2 \end{array} \right)$$

chgt de base?  $E_2 = \text{vect. propre pour la vp } 2.$

$$\begin{cases} -2x + y = 0 \\ -4x + 2y = 0 \\ -2x + y = 0 \end{cases} \Leftrightarrow y = 2x \quad \text{base} \left( \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix} \right)$$

$e_1 \qquad e_3$

On veut trouver  $e_2$  /  $f(e_2) = 2e_2 + e_3$

$e_2 \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix}$  vérifie

$$\begin{cases} \beta = 2\alpha + 1 \\ -4\alpha + 4\beta = 2\beta + 2 \\ -2\alpha + \beta + 2\gamma = 2\gamma + 1 \end{cases}$$

$$\text{d'où } e_2 = \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix}$$

$$A = \begin{pmatrix} 1 & -3 & 0 & 3 \\ -2 & -6 & 0 & 13 \\ 0 & -3 & 1 & 3 \\ -1 & -4 & 0 & 8 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1-X & -3 & 0 & 3 \\ -2 & -6-X & 0 & 13 \\ 0 & -3 & 1-X & 3 \\ -1 & -4 & 0 & 8-X \end{pmatrix}$$

$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -3 & 0 & 0 \\ 0 & 2-X & \frac{1}{3}(X^2-3X+2) & X-1 \\ 0 & 4X-7 & \frac{1}{3}(-4X^2+7X) & X^2-5X+4 \end{pmatrix}$$

$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -3 & 0 & 0 \\ 0 & 0 & \frac{1}{3}(X-1)(X-2) & X-1 \\ 0 & 0 & -\frac{4}{3}(X-1)(X-\frac{7}{4}) & (X-1)(X-4) \end{pmatrix}$$

$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -3 & 0 & 0 \\ 0 & 0 & X-1 & 0 \\ 0 & 0 & 0 & -\frac{1}{3}(X-1)^3 \end{pmatrix}$$

Invariantes de similitudes

$$1, 1, X-1, (X-1)^3$$

$$(E, u) \cong \left( \frac{K[X]}{(X-1)} \oplus \frac{K[X]}{(X-1)^3}, X \cdot \text{id} \right)$$

$$\begin{aligned} 1 &\rightarrow X \\ \overline{(X-1)} &\rightarrow X \overline{(X-1)} \\ \overline{(X-1)}^2 &\rightarrow \overline{(X-1)}^2 X \end{aligned} \quad \left\{ \begin{aligned} X &= X-1 + 1 \\ X(X-1) &= (X-1)^2 + X-1 \\ X(X-1)^2 &= (X-1)^3 + (X-1)^2 \end{aligned} \right.$$

La matrice de Jordan de  $u$  est

$$\left( \begin{array}{c|ccc} 1 & 0 & 0 & 0 \\ \hline 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{array} \right)$$

semblable à

$$\left( \begin{array}{cccc} 1 & -3 & 0 & 3 \\ -2 & -6 & 0 & 13 \\ 0 & -3 & 1 & 3 \\ -1 & -4 & 0 & 8 \end{array} \right)$$

Changement de base

$$E \cong \frac{K[X]}{(X-1)} \times \frac{K[X]}{(X-1)^3} \quad \text{Si } v = w - 1_E$$

alors  $v^3 = 0$  (cf. (x))

Retour au problème :

6

$$u \text{ diag} \Leftrightarrow u_i \text{ diag} \quad \forall i$$

$$\Leftrightarrow \begin{cases} \text{Snt } \alpha_i = \alpha_{n-i+1} = 0 \\ \text{Snt } \alpha_i \alpha_{n-i+1} \neq 0 \end{cases} \quad \forall i$$

## Décomposition p primaire.

G fini

p premier  $G_p = \{x \in G \mid \exists \alpha \mid \omega(x) = p^\alpha\}$

$G_p$  = sous-groupe de G est un p groupe.

C'est la p-composante de G  $\hat{=}$  le plus grand spgroupe de G.

$$\exists! \quad G = \prod_{p \in \mathcal{P}} G_p$$

Preuve :

$$1) \omega(x) = p^\alpha$$

$$\omega(y) = p^\beta$$

$$(xy)^{p^{\alpha+\beta}} = 1 \Rightarrow \omega(xy) \mid p^{\alpha+\beta} \Rightarrow xy \in G_p$$

$$\Rightarrow G_p \neq \emptyset \text{ car } 1 \in G_p.$$

$$\omega(x^{-1}) = \omega(x) \text{ car } \dots$$

2)  $G_p$  est un p-groupe.

$$\text{En effet : } \forall x \in G_p \quad \omega(x) = p^\alpha \Rightarrow \# G_p = p^\beta$$

Preuve :

$$G_p = \{x_1, \dots, x_n\} \quad \prod_{1 \leq i \leq n} \langle x_i \rangle = \Gamma \quad \# \Gamma = p^\gamma$$

$$\Gamma = \prod_{1 \leq i \leq n} \langle \pi_i \rangle \xrightarrow{\varphi} G_p$$

$$(y_1, \dots, y_n) \mapsto y_1 \dots y_n$$

C'est un morphisme de groupe, surjectif,

$$\begin{array}{ccc} \Gamma & \xrightarrow{\varphi} & G_p \\ \pi \downarrow & \nearrow & \\ \Gamma/H & \sim & \end{array} \quad H = \ker \varphi$$

•  $G_p \cong \Gamma/H \Rightarrow \text{Card } G_p \mid \underbrace{\text{Card } \Gamma}_{p^\beta} \Rightarrow \text{Card } G_p = p^\beta \text{ sur.}$

3)

**Important**

$G$  groupe cyclique d'ordre  $n$  ( $\#G = n$ )

Si  $d \mid n$ ,  $\exists ! G_d$  sous-groupe de  $G$  tel que  $\#G_d = d$

et  $G_d = \{x \in G / dx = 0\}$

$$(1) \quad d = \Delta(n, m) \Rightarrow X^d - 1 = \Delta(X^n - 1, X^m - 1)$$

Supposons que  $m > n$

$$(P) = (X^n - 1, X^m - 1) = (X^n - 1, X^{m-n} - 1) \quad \text{puisque} \quad \begin{array}{r} X^m - 1 \\ -X^n + X^{m-n} \\ \hline X^{m-n} - 1 \end{array} \quad \begin{array}{r} X^n - 1 \\ \hline X^{m-n} \end{array}$$

d'où

$$(P) = (X^n - 1, X^m - 1) = (X^n - 1, X^r - 1) \quad \text{où } r = m - qn$$

$$0 \leq r < n$$

$$(P) = (X^s - 1, X^r - 1) \quad \text{où } s = \text{reste de la division euclidienne de } n \text{ par } r$$

$$\begin{cases} m = q_1 n + r \\ n = q_2 r + s \\ \vdots \\ a = bc + d, \text{ dernier reste non nul, } d = \Delta(m, n) \\ c = \delta d \end{cases}$$

$$\text{d'où } (P) = (X^d - 1, X^c - 1) \quad \text{où } d \mid c$$

$$\text{Il est manifeste que } d \mid c \Rightarrow X^d - 1 \mid X^c - 1$$

$$\text{donc } (P) = (X^d - 1) \Rightarrow P = X^d - 1 = \Delta(X^n - 1, X^m - 1)$$

2<sup>e</sup> méthode : On est dans  $\mathbb{R}[X]$

$$\text{On a } \begin{cases} (X^d - 1)f = X^n - 1 \\ (X^d - 1)g = X^m - 1 \end{cases}$$

$$\text{Montrons que } \Delta(f, g) = 1$$

$$f = a \prod (X - a_i)^{\alpha_i} \quad a_i \in \mathbb{C}$$

On a :

$$\Delta(f, g) = 1 \Leftrightarrow \begin{cases} f \text{ et } g \text{ n'ont pas de racines dans } \mathbb{C} \\ \text{communes.} \end{cases}$$

( $\Rightarrow$ ) oui

( $\Leftarrow$ )  $D \mid f$  et  $D \mid g$  et  $D \in \mathbb{C}[X]$   $f$  et  $g$  n'ont pas de racines complexes communes, donc  $D = c \cdot 1$  (Théorème de d'Alembert: "Tout polynôme de  $\deg \geq 1$  admet au moins 1 racine")

Retourmons à  $\delta(f, g) = 1$ :

$$\text{Si } \alpha \in \mathbb{C} / f(\alpha) = g(\alpha) = 0 \Rightarrow \begin{cases} \alpha^n - 1 = 0 \\ \alpha^m - 1 = 0 \end{cases} \quad (1)$$

$$\exists \delta(n, m) = d \Leftrightarrow \begin{cases} d \mid n \text{ et } d \mid m \\ \text{et} \\ d = un + vm \end{cases}$$

$$\text{donc } \alpha^d = (\alpha^n)^u (\alpha^m)^v = 1$$

$\Rightarrow$

$$(1) \Rightarrow \alpha^d - 1 = 0$$

Ainsi  $X^n - 1 = (X^d - 1) f$  admet  $\alpha$  comme racine double.

Montrons que  $X^n - 1$  n'admet pas de racines doubles:

$$h = X^n - 1 \quad \alpha^n = 1$$

$$h' = nX^{n-1}$$

$$h'(\alpha) = 0 \Rightarrow n\alpha^{n-1} = 0 \Rightarrow \alpha = 0 \quad (\text{si le corps est de caractéristique } \neq n)$$

impossible.

Exo:  $k = \text{corps fini} \quad \exists f \text{ non constant } f \in k[X] \text{ qui n'a pas de racines.}$

Preuve:

$$f(x) = \prod_{i=1}^n (x - a_i) + 1 \quad \text{ou } k = \{a_1, \dots, a_n\}$$



⑤ Soit  $A = aI + J_n$  où  $(J_n)^n = 0$

$$f(x) = \sum_{k \geq 0} \frac{(x-a)^k}{k!} f^{(k)}(a) \quad (\text{Formule de Taylor pour les polynômes})$$

Appliqué en  $A \in \mathbb{K}[X]$

$$f(A) = f(aI + J_n) = \sum_{k=0}^{\infty} \frac{J_n^k}{k!} f^{(k)}(a) = f(a) + \dots + \frac{J_n^{n-1}}{(n-1)!} f^{(n-1)}(a)$$

Remarque: On définit :

$$e^A = \sum_{k=0}^{\infty} \frac{A^k}{k!} = f(A) \in \mathcal{M}(n \times n) \text{ car la série converge uniformément (c.à.d pour } \|\cdot\|_F) \text{ et } \mathcal{M}(n \times n) = \text{Banach.}$$

On trouve, par un m calcul :

$$e^A = \begin{pmatrix} e^a & e^a & \dots & \frac{e^a}{(n-1)!} \\ & e^a & \dots & e^a \\ & & \ddots & e^a \\ 0 & & & e^a \end{pmatrix} = e^a \begin{pmatrix} 1 & 1 & \dots & 1 \\ & 1 & \dots & 1 \\ & & \ddots & 1 \\ 0 & & & 1 \end{pmatrix}$$

$$\det e^A = e^{na}$$

$$\text{tr } e^A = na$$

Remarque : On a toujours  $\boxed{\det e^A = e^{\text{tr } A}}$   $\forall A$  matrice  $\mathcal{M}(n \times n)$

En effet,  $A$  est décomposable en blocs de Jordan  $\begin{pmatrix} A_1 & & \\ & A_i & \\ & & \ddots \\ & & & A_n \end{pmatrix}$

$$\begin{cases} \text{tr } A = \sum \text{tr } A_i \\ \det A = \prod \det A_i \end{cases}$$

$$\text{On a } e^A = \begin{pmatrix} e^{A_1} & & \\ & \ddots & \\ & & e^{A_n} \end{pmatrix} \Rightarrow \det e^A = \prod \det e^{A_i} = \prod e^{\text{tr } A_i} = e^{\sum \text{tr } A_i} = e^{\text{tr } A} \quad \text{CQFD}$$

## Feuille N° 8

x1° Quels sont les polynômes irréductibles de degrés 2 et 3 à coefficients dans  $\mathbb{F}_2$ ? Donner des tables de multiplication de  $\mathbb{F}_4$ ,  $\mathbb{F}_8$ ,  $\mathbb{F}_9$ .

x2° Soit  $A$  une  $\mathbb{R}$ -algèbre de dimension 2 (i.e. un anneau muni d'une structure de  $\mathbb{R}$ -espace vectoriel dont la loi de groupe est celle de l'anneau). Soit  $\{1, e\}$  une base de  $A$ . Montrer qu'il existe un polynôme  $f \in \mathbb{R}[X]$  de degré 2 vérifiant  $f(e) = 0$ . En déduire que  $A$  est isomorphe à l'une des trois algèbres suivantes :  $\mathbb{R} \times \mathbb{R}$  avec la loi  $(x, y)(x', y') = (xx', yy')$ ,  $\mathbb{R}[X]/(X^2)$  (nombres duaux, ou développements limités au deuxième ordre),  $\mathbb{C}$ .

x3° Soit  $f \in \mathbb{Q}[X]$  le polynôme  $X^3 - 2$ .

a) montrer que  $f$  est irréductible.

b) montrer que le plus petit sous-corps de  $\mathbb{R}$  contenant  $\sqrt[3]{2}$  est le corps de rupture de  $f$ ; on le note  $\mathbb{Q}(\sqrt[3]{2})$ . Écrire explicitement les éléments de  $\mathbb{Q}(\sqrt[3]{2})$ ; calculer  $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2})$ .

c) Quel est le corps de décomposition  $K$  de  $f$ ? a-t-on  $\mathbb{Q}$

$K = \mathbb{Q}(\sqrt[3]{2})$ ? Calculer  $\dim K$ .

(2)

x 4° Soient  $L$  un corps fini,  $k$  un sous-corps de  $L$ ,  $\xi$  un générateur de  $(L^*, x)$ .

a) montrer que le plus petit sous-corps de  $L$  contenant  $k$  et  $\xi$  est  $L$

b) On définit  $\varphi: k[x] \rightarrow L$  par  $\varphi(f) = f(\xi)$ . Alors

i)  $\varphi$  est un morphisme surjectif d'anneaux.

ii) il existe un polynôme irréductible  $f \in k[x]$  vérifiant

$$f(\xi) = 0 \text{ et } L \simeq k[x]/f k[x]$$

c) Montrer que si  $k$  est un corps fini,  $n$  un entier au moins égal à 2, il existe un polynôme irréductible de degré  $n$  dans  $k[x]$ .

5° Soit un nombre premier  $p$  et soit un corps  $\mathbb{F}_q$  de caractéristique  $p$ ,  $n > 0$  un entier premier avec  $p$ . Soit  $k$  le corps des racines de  $X^n - 1$  sur  $\mathbb{F}_q$ .

a) Montrer que  $n \mid (\#k - 1)$

b) Montrer que  $k = \mathbb{F}_{q^m}$  où  $m = \min \left\{ \lambda \in \mathbb{N}^* \mid \frac{\lambda}{n} | q^\lambda - 1 \right\}$

c) Conclure que si  $p$  est premier, si  $\lambda \in \mathbb{N}^*$ ,  $n \in \mathbb{N}^*$  et  $(p, n) = 1$ , il existe  $m \in \mathbb{N}^*$  vérifiant  $n \mid p^{\lambda m} - 1$ . Que se passe-t-il si  $p$  n'est pas premier?

$$\textcircled{1} \quad p \in \mathcal{P} \quad n \in \mathbb{N}^*$$

$\mathbb{F}_{p^n}$  = corps à  $p^n$  éléments

Lemme ( $K = \text{corps}$ )

$2 \leq \deg f \leq 3 \quad f \text{ irréductible dans } K \Leftrightarrow f \text{ n'a pas de racine dans } K.$

important

Preuve :  $f \text{ non irréductible} \Leftrightarrow f = gh \quad \begin{cases} \deg h \geq 1 \\ \deg g \geq 1 \end{cases}$

et  $\deg f = 2 \Rightarrow \deg h = 1 \quad \deg g = 1 \Rightarrow f \text{ possède une racine.}$

et  $\deg f = 3 \Rightarrow h \text{ ou } g \text{ est de degré } 1 \Rightarrow f \text{ possède une racine.}$

L'équivalence en résulte.

$$1^\circ \quad \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$$

$X^2 + aX + b$  4 polynômes de degré 2.

$X^2 + X + 1$	→ irréductible
$X^2 + 1$	
$X^2$	
$X^2 + X$	

Si le polynôme est de degré 3 :

$$P = X^3 + aX^2 + bX + c \quad 8 \text{ choix}$$

Préductible  $\Leftrightarrow P$  admet une racine (0 ou 1)

Si cette racine est 0, alors  $c = 0$ ,  $P = X^3 + aX^2 + bX$  soit 4 choix possibles.

Si cette racine est 1,  $1 + a + b + c = 0 \Leftrightarrow (a, b, c) = (0, 1, 0)$  i.e.  $c = 0$ .

$$(1, 0, 0)$$

$$(0, 0, 1)$$

$$(1, 1, 1)$$

Deux triplets  $(0,1,0)$  et  $(1,0,0)$  sont à écarter puisqu'ils ont déjà été comptés (cf.  $c=0$ ).

En conclusion, il y a 6 réductibles sur 8.

En conclusion :

P de deg 2 : 1 irréductible sur 4 (dans  $\mathbb{F}_2$ )  
P de deg 3 : 2 " sur 8

27

On rappelle que :

$f \in \mathbb{K}[X]$  irréductible  $\Rightarrow \mathbb{K}[X]/(f)$  corps  
(corps de rupture de  $\mathbb{K}$ )

Si  $\mathbb{K}$  est fini, on a  $\# \text{Card} \left( \mathbb{K}[X]/(f) \right) = (\text{Card } \mathbb{K})^{\deg f}$

et que : tous les corps  $\mathbb{F}_q$  à  $q$  éléments sont isomorphes, en tant que corps, entre eux.

$X^2 + X + 1$  est irréductible dans  $\mathbb{F}_2$

Ainsi :

$\mathbb{F}_2[X]/(X^2 + X + 1) = \{0, 1, \dot{X}, \dot{X}^2\}$   
ce sont bien 4 éléments distincts.

$$\begin{aligned} \text{On a } \dot{X} \cdot \dot{X}^2 &= X^3 = X(X^2 + X + 1) = X^3 + X^2 + X \\ &= +X^2 + X = 1 \end{aligned}$$

Tables de multiplication de  $\mathbb{F}_8$

On fait de même ;

$$\mathbb{F}_2[X] / (X^3 + X + 1) = \{0, 1, X, X^2, X^3, X^4, X^5, X^6\}$$

tous distincts

(possède  $2^3 = 8$  éléments)

$$\alpha : X^7 = X^6 \cdot X = 1$$

On connaît la table de multiplication du corps  $\mathbb{F}_2[X] / (X^3 + X + 1)$  à 8 éléments.

$$\mathbb{F}_9$$

$$\beta \in \mathbb{F}_3[X] \quad \deg \beta = 2 \quad X^2 + aX + b \quad \begin{array}{l} a \in \{-1, 0, 1\} \\ b \in \{-1, 1\} \end{array}$$

On en choisit un qui soit irréductible : On a le choix entre

$$\left\{ \begin{array}{l} X^2 + X + 1 \\ X^2 + 1 \\ X^2 + X - 1 \\ X^2 - X - 1 \end{array} \right.$$

(et les mêmes multipliées par  $(-1)$ )

$$\text{Donc } \mathbb{F}_9 \simeq_{\text{corps}} \mathbb{F}_3[X] / (X^2 + 1)$$

(2)  $A = \mathbb{R}$ -algèbre de dimension 2.  $\begin{cases} (A, +, \cdot) \text{ ev} \\ (A, +, \times) \text{ anneau} \\ \lambda(x \times y) = (\lambda x) \times y = x \times (\lambda y) \end{cases}$

Par exemple (1),  $\mathbb{R}[X]/(X^2) = \text{"nombres duaux"} = \{a + b\varepsilon, \text{ où } \varepsilon^2 = 1\}$ ,  $\mathbb{R} \times \mathbb{R}$

Exercice ;  $B = C_{\mathbb{R}}^{\infty}[-1, 1]$

$$I = \{f \in B / f(0) = \dots = f^{(n)}(0) = 0\} \text{ idéal de } B$$

$$(B, I) \Leftrightarrow (\mathbb{R}[X], (X^{n+1}))$$

On peut dire que  $B/I \simeq \mathbb{R}[X]/(X^{n+1})$

En effet :

$$\begin{array}{ccc} B & \xrightarrow{\text{homomorphisme surj. d'anneaux}} & \mathbb{R}[X]/(X^{n+1}) \\ b & \longmapsto & \text{classe de } \left( \sum_{k=0}^n \frac{b^{(k)}(0)}{k!} X^k \right) \\ \downarrow & \nearrow \text{isomorphisme} & \\ B/I & & \end{array}$$

A de base  $\{1, e\}$

Trouver  $f$  /  $\deg f = 2$  /  $f(e) = 0$ .

Prenons  $f(X) = X^2 + bX + c$

$$f(e) = 0 \Leftrightarrow e^2 + be + c = 0$$

$$\Leftrightarrow e^2 = -c - be$$

Ainsi :  $e^2 = a \cdot 1 + b \cdot e$   $a, b \in \mathbb{R}$

$$f(X) = X^2 - bX - a \Rightarrow f(e) = 0$$

③ Considérons

$$\begin{aligned} \mathbb{R}[X] &\xrightarrow{\varphi} A \\ g &\mapsto g(e) \end{aligned}$$

$\varphi =$  homomorphisme  
d'algèbre surjectif  
de noyau  $\ker \varphi = \{h\}$

En effet  $\forall a \in A$  :  $a = \alpha \cdot 1 + \beta e = (\alpha + \beta X)(e)$

On a  $(\beta) \subset \ker \varphi$  puisque  $\beta(e) = 0$ .

Montrons que  $(\beta) = \ker \varphi$ .

Lemme:  $\left. \begin{array}{l} g \in \mathbb{R}[X] \setminus \{0\} \\ \deg g = 0 \text{ ou } 1 \end{array} \right\} \Rightarrow g(e) \neq 0 \quad (\text{facile})$

d'où  $\deg h = \inf \{ \deg m \mid m \in \ker \varphi \} \geq 2$  et  $\beta \in \ker \varphi$   $\deg \beta = 1$ .

Donc  $\ker \varphi = (\beta)$ . oui

Tout cela pour :

$$\begin{array}{ccc} \mathbb{R}[X] & \xrightarrow{\varphi} & A \\ g & \mapsto & g(e) \\ \pi \downarrow & \nearrow \sim \text{d'algèbre} & \\ \mathbb{R}[X]/(\beta) & & \end{array}$$

Ainsi :  $A \underset{\text{alg}}{\simeq} \mathbb{R}[X]/(\beta)$

De 3 choses l'une :

1)  $\beta$  n'a pas de racines.

$$\beta(X) = (X + \alpha)^2 + \beta^2 \quad \alpha, \beta \in \mathbb{R}$$



$$\begin{array}{ccc}
 \mathbb{R}[X] / (f) & \xrightarrow{\sim \Psi} & \mathbb{C} \\
 \uparrow & \nearrow g(\beta i - \alpha) & \\
 \mathbb{R}[X] & \xrightarrow{\Psi} & \mathbb{C}
 \end{array}
 \quad \left. \begin{array}{l} \\ \end{array} \right\} \begin{array}{l} \text{car } \left( \frac{X+\alpha}{\beta} \right)^2 + 1 = 0 \\ \text{donc } \Psi\left(\frac{X+\alpha}{\beta}\right) = i \end{array}$$

$\Psi = \text{homomorphisme d'alg\`ebre.}$   
 (c'est le complexe "polynome en un point")

$$\text{Ker } \Psi = \{ g \in \mathbb{R}[X] / g(\beta i - \alpha) = 0 \}$$

Si  $g(\beta i - \alpha) = 0$ , alors  $g(-\beta i + \alpha) = 0$ , et donc

$$(X - \beta i + \alpha)(X + \beta i + \alpha) \mid g$$

①

$$(X + \alpha)^2 + \beta^2 \mid g$$

②

$$g = 0 \text{ dans } \mathbb{R}[X] / (f)$$

Donc  $\text{Ker } \Psi = (f)$ .

Enfin,  $\Psi$  est surjective car

$$\begin{cases} \Psi(1) = 1 \\ \Psi\left(\frac{X+\alpha}{\beta}\right) = i \end{cases}$$

En conclusion  $A \underset{\text{alg}}{\simeq} \mathbb{R}[X] / (f) \underset{\text{alg}}{\simeq} \mathbb{C}$

2)  $\Delta = 0$

$$\begin{array}{ccc}
 \mathbb{R}[X] / (f) & \xrightarrow{\sim \bar{\Psi}} & \mathbb{R}[X] / (X^2) \\
 \uparrow & \nearrow g(X+\alpha) & \\
 \mathbb{R}[X] & \xrightarrow{\Psi} & \mathbb{C}
 \end{array}$$

(puisque  $(X - \alpha)^2 \xrightarrow{\Psi} 0$ )  
 donc  $\Psi(X) = (X - \alpha)$

### 3) 2 racines distinctes

$$\begin{array}{ccc} \mathbb{R}[X] / (f) & \xrightarrow{\bar{\Psi}} & \mathbb{R} \times \mathbb{R} \\ \uparrow & \nearrow \Psi & \\ \mathbb{R}[X] & & (g(\alpha), g(\beta)) \end{array}$$

(ancienne méthode en rouge)

$\Psi$  morph. de  $\mathbb{R}$ -algèbre, de noyau  $\text{Ker } \Psi = (f)$ .

$\Psi$  est surjective : trouver  $g / \begin{cases} g(\alpha) = 1 \\ g(\beta) = 0 \end{cases}$  et  $h / \begin{cases} h(\alpha) = 0 \\ h(\beta) = 1 \end{cases}$

Remarque :

$$f(X) = (X - \alpha)(X - \beta) \quad \alpha \neq \beta$$

$$\frac{X - \beta}{\alpha - \beta}$$

$$\frac{X - \alpha}{\beta - \alpha}$$

(théorème chinois)

$$\bullet \quad \mathbb{R}[X] / (f) \underset{\text{anneaux}}{\simeq} \mathbb{R}[X] / (X - \alpha) \times \mathbb{R}[X] / (X - \beta)$$

et

$$\mathbb{R}[X] / (X - \alpha) \simeq \mathbb{R}$$

$$h \mapsto h(\alpha)$$

Mais on avait seulement un morphisme d'anneaux. Il y a encore à travailler.

Conclusion : Il n'y a que 3 structures de  $\mathbb{R}$ -algèbre de dimension 2, à isomorphisme près, bien sûr.

$$A \simeq_{\text{alg.}}$$

⊗ Remarque:

$$\alpha \in \mathbb{C} \text{ racine de } X^3 + X + 1 = 0$$

$$\beta \in \mathbb{C} \text{ " } X^2 + X - 3 = 0$$

$$P, Q \in \mathbb{Q}[X] \quad \left\{ \begin{array}{l} P(\alpha) = 0 \\ Q(\beta) = 0 \end{array} \right. \quad \alpha, \beta \in \mathbb{C} \quad \Rightarrow \quad \left\{ \begin{array}{l} U(X) = P(X - \beta) \text{ de racine } \alpha + \beta \\ V(X) = Q(X - \alpha) \text{ " } \end{array} \right.$$

Résultant de  $f$  et  $g$

Th |  $f, g \in \mathbb{K}[X]$   
 $\text{Res}(f, g) = \text{nombre qui s'exprime comme un polynôme à coefficients}$   
entiers en les coefficients de  $f$  et  $g$

Pr |  $f$  et  $g$  ne sont pas premiers entre eux  
 $\Updownarrow$   
 $\text{Res}(f, g) = 0$

} coefficients de  $U = \text{polyn. en } \beta$  à coefficients dans  $\mathbb{Q}$

On prendra plutôt

$$\left\{ \begin{array}{l} U(X) = P\left(X + \frac{\alpha + \beta}{2}\right) \\ V(X) = Q\left(-X + \frac{\alpha + \beta}{2}\right) \end{array} \right. \quad \begin{array}{l} U\left(\frac{\alpha - \beta}{2}\right) = 0 \\ V\left(\frac{\alpha - \beta}{2}\right) = 0 \end{array}$$

On calcule le résultant de  $U$  et  $V$ , qui est nul. (cf. Th.) et c'est un polynôme en  $\alpha + \beta$  à coeff. entiers.

X

# Résultant

$$\begin{cases} d = \deg P \\ e = \deg Q \end{cases}$$

$$S_k = \{f \in K[X] / \deg f < k\}$$

$$S_d \oplus S_e \xrightarrow{\Phi} S_{d+e}$$

$$(u, v) \rightarrow uQ + vP$$

$\Phi$  est linéaire.

$$\Phi \text{ surjective} \Rightarrow \exists u, v / uP + vQ = 1 \Rightarrow \Delta(P, Q) = 1.$$

$$\bullet \Delta(P, Q) = 1 \Rightarrow \Phi \text{ injective car } uQ = -vP \Rightarrow P|u \Rightarrow u=0 \Rightarrow v=0. \\ \Rightarrow \Phi \text{ bijective (espaces ont m dimension)}$$

$$\text{Ainsi : } \Phi \text{ isomorphisme} \Leftrightarrow \Delta(P, Q) = 1$$

$$\begin{cases} S_d \oplus S_e \text{ de base } (1, 0) (X, 0) \dots (X^{d-1}, 0) (0, 1) \dots (0, X^{e-1}) \\ S_{d+e} \text{ de base } 1 \ X \dots X^{d+e-1} \end{cases}$$

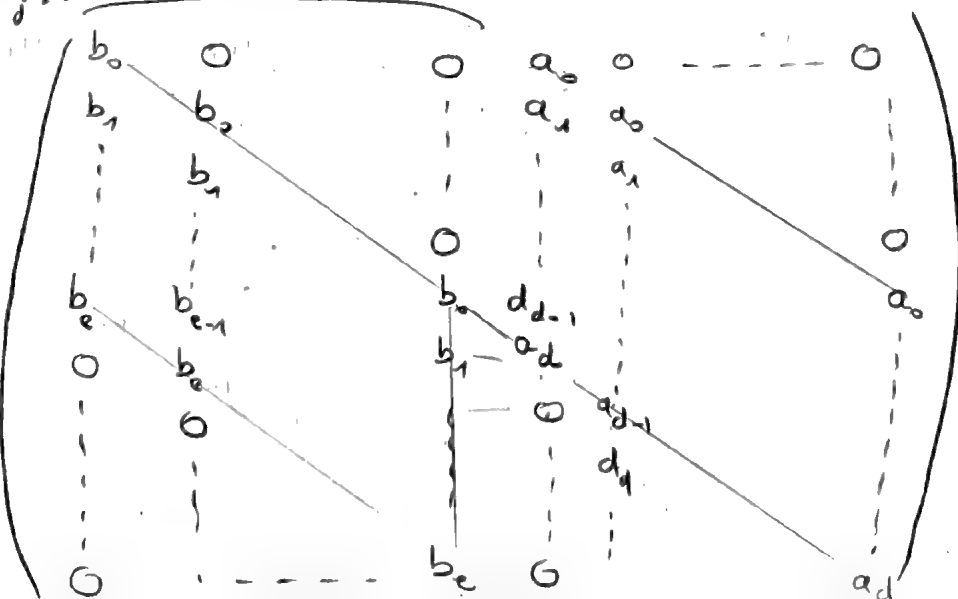
Exprimons  $\Phi$  dans ces bases;

$$\begin{cases} P = \sum_{i=0}^d a_i X^i \\ Q = \sum_{j=0}^e b_j X^j \end{cases}$$

d colonnes

mat  $\Phi =$

d-1 lignes



Application: (cf. feuille 4 de ce TD).

$$\begin{cases} P = X^3 + X + 1 & P(\alpha) = 0 \\ Q = X^2 + X - 3 & P(\frac{\beta}{Q}) = 0 \end{cases}$$

On a :

$$\text{Res} \left( \underbrace{P\left(X + \frac{\alpha + \beta}{2}\right)}_U, \underbrace{Q\left(-X + \frac{\alpha + \beta}{2}\right)}_V \right) = 0 \quad \text{car } \Delta(U, V) \neq 0.$$

$$u = \alpha + \beta$$

$$\begin{aligned} P\left(X + \frac{u}{2}\right) &= X^3 + 3X^2 \frac{u}{2} + 3X \frac{u^2}{4} + \frac{u^3}{8} + X + \frac{u}{2} + 1 \\ &= \frac{1}{8} \left[ 8X^3 + 12uX^2 + (6u^2 + 8)X + u^3 + 4u + 8 \right] \end{aligned}$$

ne servira à rien pour l'annulation du résultant.

$$Q\left(-X + \frac{u}{2}\right) = X^2 + \frac{u^2}{4} - uX - X + \frac{u}{2} - 3$$

$$Q\left(-X + \frac{u}{2}\right) = \frac{1}{4} \left[ 4X^2 - 4(u+1)X + u^2 + 2u - 12 \right]$$

$$\det \begin{pmatrix} 8 + 4u + u^3 & 0 & -12 + 2u + u^2 & 0 & 0 \\ 8 + 6u^2 & 8 + 4u + u^3 & -4(u+1) & -12 + 2u + u^2 & 0 \\ 12u & 8 + 6u^2 & 4 & -4(u+1) & -12 + 2u + u^2 \\ 8 & 12u & 0 & 4 & -4(u+1) \\ 0 & 8 & 0 & 0 & 4 \end{pmatrix}$$

$$(3) f \in \mathbb{Q}[X] \quad f = X^3 - 2$$

$$a) \frac{p^3}{q^3} - 2 = 0 \Leftrightarrow p^3 - 2q^3 = 0 \Rightarrow q \mid p \quad (\text{car } \delta(p, q) = 1)$$

donc  $q = 1$  (on peut prendre  $q > 0$ )

Alors  $p^3 = 2 \Rightarrow p = \pm 1$  ou  $\pm 2$ . Aucune de ces valeurs ne convient.

Donc :  $f$  n'admet pas de racines rationnelles.

Le lemme suivant permet de conclure :

Lemme :  $K = \text{corp.}$

$P \in K[X] / \deg P = 2 \text{ ou } 3$

(important)

Alors  $P$  irréductible sur  $K[X] \Leftrightarrow \nexists x \in K / P(x) = 0$

$$b) \mathbb{Q}(\sqrt[3]{2}) \underset{\substack{\cong \\ \text{corp.}}}{=} \mathbb{Q}[X] / (X^3 - 2)$$

$\mathbb{Q}(\sqrt[3]{2})$  est un espace vectoriel de dimension 3 sur  $\mathbb{Q}$ , de base  $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$

$$\mathbb{Q}(\sqrt[3]{2}) = \left\{ a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q} \right\}$$

$$\bullet \text{ sur } \mathbb{Q} \quad \dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}) = 3$$

c)

$$\text{On a } K = \mathbb{Q}(\sqrt[3]{2})$$

$$X^3 - 2 = (X - \sqrt[3]{2})(X^2 + X\sqrt[3]{2} + 2^{\frac{2}{3}}) \quad \text{dans } \mathbb{Q}(\sqrt[3]{2})[X]$$

Le polynôme  $(X^2 + \sqrt[3]{2}X + 2^{\frac{2}{3}})$  est-il irréductible dans  $\mathbb{Q}(\sqrt[3]{2})[X]$  ?

S'il ne l'est pas, il existe  $x = a + b\sqrt[3]{2} + c\sqrt[3]{4}$  racine de ce polynôme :

$$(a + b2^{\frac{1}{3}} + c2^{\frac{2}{3}})^2 + 2^{\frac{1}{3}}(a + b2^{\frac{1}{3}} + c2^{\frac{2}{3}}) + 2^{\frac{2}{3}} = 0 \quad a, b, c \in \mathbb{Q}$$

d'où

$$a^2 + 4bc + 2c + 2^{\frac{1}{3}}(a + 2ab + 2c^2) + 2^{\frac{2}{3}}(1 + 2ac + b^2 + b) = 0$$

$$\begin{cases} a^2 + 4bc + 2c = 0 & (1) \\ a + 2ab + 2c^2 = 0 & (2) \\ 1 + 2ac + b + b^2 = 0 & (3) \end{cases}$$

$$(3) \Rightarrow 2c(1 + 2b) = -a^2 \Rightarrow 4c^2(1 + 2b)^2 = a^4$$

$$\text{or } (2) \Rightarrow 2c^2 = -a(1 + 2b) \text{ d'où } a[a^3 + 2(1 + 2b)^3] = 0$$

$$a \neq 0 \text{ car } a = 0 \Rightarrow c = 0 \Rightarrow b^2 + b + 1 = 0 \text{ et } b \in \mathbb{Q}, \text{ faux.}$$

$$\text{donc } a \neq 0 \Rightarrow a^3 + 2(1 + 2b)^3 = 0 \Rightarrow \frac{a^3}{(1 + 2b)^3} + 2 = 0$$

impossible sur  $\mathbb{Q}$  car  $X^3 + 2$  est irréductible sur  $\mathbb{Q}$

Donc  $X^3 + 2^{\frac{1}{3}}X + 2^{\frac{2}{3}}$  est irréductible sur  $\mathbb{Q}(\alpha)$   $\alpha = \sqrt[3]{2}$

Conclusion :

$$\boxed{K \neq \mathbb{Q}(\sqrt[3]{2})}$$

dimension 3

$\dim_{\mathbb{Q}} K$  ?

$$F = \frac{\mathbb{Q}(\alpha)[X]}{(X^3 + 2^{\frac{1}{3}}X + 2^{\frac{2}{3}})} = \text{corps de rupture du polynôme } X^3 + 2^{\frac{1}{3}}X + 2^{\frac{2}{3}} \quad (\text{par ex. } \beta = j\alpha)$$

$$\dim_{\mathbb{Q}(\alpha)} F = 2$$

$$\forall f \in F \quad f = a + bX + cX^2 \quad a, b, c \in \mathbb{Q}(\alpha)$$

$$X \equiv \beta$$

$$\forall f \in F \quad f = (a_1 + a_2\alpha) + (b_1 + b_2\alpha)\beta \quad \beta = j\alpha$$

$$\beta \in F \Leftrightarrow \beta = \overbrace{a_1 + a_2 \alpha + a_3 \alpha^2 + b_1 \beta + b_2 \alpha \beta + b_3 \alpha^2 \beta}^{a_i + a_2 \alpha + a_3 \alpha^2 + b_1 \beta + b_2 \alpha \beta + b_3 \alpha^2 \beta} \quad (\alpha \beta = j \alpha^2)$$

$$a_i, b_i \in \mathbb{Q}$$

$$\dim_{\mathbb{Q}} F = [F; \mathbb{Q}(\alpha)] \times [\mathbb{Q}(\alpha); \mathbb{Q}]$$

$$\dim_{\mathbb{Q}} F = 2 \times 3 = 6$$

donc

On a  $F = K =$  corps des racines de  $f$

Car, si  $\alpha, \beta, \gamma$  sont les 3 racines de  $f$  dans  $G$ ,

$$F = \mathbb{Q}(\alpha, \beta) \underset{\text{évident}}{=} \mathbb{Q}(\alpha)(\beta)$$

$$\text{puisque } \mathbb{Q}(\alpha)(\beta) = \mathbb{Q}(\alpha)[X] / (X^2 + 2^{\frac{1}{3}}X + 2^{\frac{2}{3}})$$

$$\text{En effet, } f(X) = X^3 - 2 = \underbrace{(X - \alpha)}_{\in F[X]} \underbrace{(X - \beta)}_{\in F[X]} Q(X) \quad \deg Q = 1$$

La dernière racine appartient donc à  $F$ .

$F$  est donc un corps de factorisation de  $f(X)$ . Montrons que c'est le corps des racines de  $f(X)$ , c.à.d que

$$\text{si } \Sigma = \text{corps tel que } \begin{cases} \mathbb{Q} \subset \Sigma \subset F \\ \Sigma \text{ de factorisation de } f(X) \end{cases} \text{ alors } \Sigma = F$$

$$\alpha, \beta \in \Sigma \text{ et } \mathbb{Q} \subset \Sigma \Rightarrow \underbrace{\mathbb{Q}(\alpha, \beta)}_F \subset \Sigma \Rightarrow F \subset \Sigma$$

Donc  $F = K$  est de dimension 6 sur  $\mathbb{Q}$



## Corps de rupture

Rappels : le plus petit sous-corps de  $\mathbb{R}$  contenant  $\sqrt[3]{2}$  est le corps de rupture de  $f$

Déterminer  $\mathbb{Q}(\sqrt[3]{2})$

On rappelle le diagramme

$$\begin{array}{ccc} \mathbb{Q}[X] & \xrightarrow{\varphi} & \mathbb{Q}(\sqrt[3]{2}) \\ P \downarrow & \xrightarrow{\quad} & P(\sqrt[3]{2}) \\ \mathbb{Q}[X]/(X^3-1) & \nearrow \bar{\varphi} & \end{array}$$

$\bar{\varphi}$  est un isomorphisme d'algèbre.

$$\text{donc } \dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}) = \dim_{\mathbb{Q}} \mathbb{Q}[X]/(X^3-1) = 3$$

et  $\bar{\varphi}(1, X, X^2)$  est une base de  $\mathbb{Q}[X]/(X^3-1)$ . Donc  $(\bar{\varphi}(1), \bar{\varphi}(X), \bar{\varphi}(X^2))$  est une base de  $\mathbb{Q}(\sqrt[3]{2})$  comme espace vectoriel sur  $\mathbb{Q}$ .

$$\begin{cases} \bar{\varphi}(1) = \varphi(1) = 1 \\ \bar{\varphi}(X) = \varphi(X) = \sqrt[3]{2} \\ \bar{\varphi}(X^2) = \varphi(X^2) = (\sqrt[3]{2})^2 \end{cases}$$

d'où 
$$\mathbb{Q}(\sqrt[3]{2}) = \left\{ a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Q} \right\}$$

Remarque:  $\text{Gal}(\mathbb{Q}(\alpha, j\alpha)/\mathbb{Q}) = \text{Aut}(\underbrace{\mathbb{Q}(\alpha, j\alpha)}_K)$

Soit  $\sigma \in \text{Aut}(K)$

Si  $x \in K$   $\lambda \in \mathbb{Q}$   $\sigma(\lambda x) = \lambda \sigma(x)$

Si  $\xi$  est racine de  $f \in \mathbb{Q}[X]$ , alors  $\sigma(\xi)$  aussi. En effet, si  $f(x) = \sum a_k x^k$

$$f(\xi) = \sum a_k \xi^k \Rightarrow f(\sigma(\xi)) = \sum a_k (\sigma(\xi))^k = \sigma(\sum a_k \xi^k) = \sigma(0) = 0$$

car  $\sigma$  est un morphisme de corps ( $\Rightarrow \sigma$  est  $\mathbb{Q}$ -linéaire)

Posons:  $\Phi: \text{Gal}(K) \rightarrow \mathcal{I}\{\alpha, \beta, \gamma\}$   $\alpha, \beta, \gamma$  racines de  $f$   
 $\sigma \mapsto \sigma|_{\{\alpha, \beta, \gamma\}}$

Alors  $\Phi$  est injective: En effet, si  $\sigma|_{\{\alpha, \beta, \gamma\}} = \sigma'|_{\{\alpha, \beta, \gamma\}}$

le base  $(1, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta)$  est transformée en  $\mathcal{B}'$  par  $\sigma$  et par  $\sigma'$  morphismes de corps. Donc  $\sigma = \sigma' \Rightarrow \Phi$  est injective.

On peut écrire

$$\Phi: \text{Gal}(K) \hookrightarrow \mathcal{I}\{\alpha, \beta, \gamma\}$$

$\uparrow$   
(Résultat général)

En particulier, si  $f = X^3 - 2$ , montrons que  $\Phi$  est surjective.

$$\begin{cases} \alpha = \sqrt[3]{2} \\ \beta = j\alpha \\ \gamma = j^2\alpha \Rightarrow \gamma = \beta^2\alpha^{-1} \end{cases}$$

Soit  $\theta \in \mathcal{I}\{\alpha, \beta, \gamma\}$ , alors considérons  $\sigma \in \text{Gal}(K)$  défini par:

$$\sigma: \begin{array}{cccccc} 1 & \alpha & \alpha^2 & \beta & \alpha\beta & \alpha^2\beta \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & \theta(\alpha) & \theta(\alpha)^2 & \theta(\beta) & \theta(\alpha)\theta(\beta) & \theta(\alpha)^2\theta(\beta) \end{array}$$

$\sigma$  est une autom application  $\mathbb{Q}$ -linéaire. En fait, c'est un automorphisme

des corps  $\mathbb{Q}(a, aj)$  : pour le montrer, nous aurons affaire à des calculs compliqués.

- ④ a) trivial  
b) Facile (le faire!)

Remarque :

$I \subset A$   $A$  anneau

$$\underline{I \text{ premier}} \Leftrightarrow A/I \text{ int\`egre} \Leftrightarrow \forall x, y \in A \quad xy \in I \Rightarrow x \text{ ou } y \in I$$

Avant :  $\underline{I \text{ maximal}} \Rightarrow I \text{ premier}$

$$\begin{array}{c} \Downarrow \\ A/I = \text{corps} \end{array} \nearrow$$

$$\underline{I \text{ principal}} \Leftrightarrow \exists a \in A/I = (a) \quad \text{I int\`egre et } \forall \text{ id\`eal } J \subset I$$

~~Pro~~ Si  $A$  est principal, alors  $I \text{ premier} \Rightarrow I \text{ maximal}$

Pro | Soit  $A$  un anneau principal  
Si  $I$  premier dans  $A$ , ~~alors~~  $I = (p)$  où  $p =$  ~~premier~~ irréductible

Def |  $p \in A$  est dit ~~premier~~ irréductible ssi  $p = uv \quad u, v \in A \Rightarrow u \text{ ou } v \in A^*$ .

~~Pro~~

Preuve de la Pro :

$$(\Leftarrow) \quad p = uv \Rightarrow p | uv \Rightarrow p | u \text{ ou } p | v \Rightarrow p$$

$$\text{Par exemple } p | u \Leftrightarrow u = \lambda p \Rightarrow 1 = \lambda v \Rightarrow v \in A^* \quad \Leftarrow$$

c)

$p$  premier  
entier  $\} \Rightarrow \exists !$  corps à  $p^n$  éléments  $\mathbb{F}_{p^n}$

1)  $\mathbb{F}_{p^n} \hookrightarrow \mathbb{F}_{q^m}$  morphisme de corps  $q=p$   $n \leq m$

$(\mathbb{F}_{p^n}^*, x) \hookrightarrow (\mathbb{F}_{q^m}^*, x) \Rightarrow$  (Lagrange)  $p^n - 1 \mid p^m - 1 \Rightarrow n \mid m$

En conclusion

•  $\mathbb{F}_{p^n} \hookrightarrow \mathbb{F}_{q^m} \Rightarrow \boxed{\begin{array}{c} p=q \\ \vee \\ n \mid m \end{array}}$

2)  $\mathbb{F}_{p^m}$  est muni d'une structure de  $\mathbb{F}_{p^n}$ -ev si  $\mathbb{F}_{p^n} \hookrightarrow \mathbb{F}_{q^m}$   $q=p$   $n \leq m$ .

$\mathbb{F}_{p^m}$  est de dimension finie, donc :

$$\begin{aligned} \exists d \in \mathbb{N} / \quad \# \mathbb{F}_{p^m} &\simeq (\# \mathbb{F}_{p^n})^d \\ p^m &= p^{nd} \\ \Downarrow \\ m &= nd \\ \Downarrow \\ n &\mid m \end{aligned}$$

(Remarque : la démonstration est faite au 1) ~~et nous~~ suppose même de connaissances)

Réciproquement ? voir (\*1)

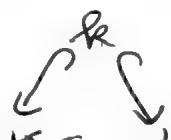
On rappelle que :  $K$  corps  $f \in K[X]$

$K \supset K$  est corps des racines  $\Leftrightarrow \left\{ \begin{array}{l} f \text{ se décompose et} \\ K = \text{le plus petit sous-corps} \\ \text{contenant les racines de } f \end{array} \right.$

(\*2)

Pro Si il existe un corps  $L$  de décomposition de  $f \in K[X]$

Alors il existe un morphisme injectif  $K \hookrightarrow L$ , c.-à.-d.



Preuve:

$\xi_1, \dots, \xi_n$  = racines de  $f$  dans  $L$

Considérons  $k(\xi_1, \dots, \xi_n) = K'$ . C'est un corps des racines de  $\mathbb{K}[X]$

D'après l'unicité (à isomorphisme près) du corps des racines:

$$\begin{array}{ccc} K & \xrightarrow{\sim} & K' \\ & \downarrow & \\ & L & \end{array}$$

d'où  $K \xrightarrow[\text{morph. inj. de corps.}]{\hookrightarrow} L$  CQFD

On rappelle que  $\mathbb{F}_p \hookrightarrow \mathbb{F}_{p^n} = \text{corps des racines de } X^{p^n} - X \in \mathbb{F}_p[X]$

(\*) Hypothèse:  $m = nd$

$$\begin{aligned} \# \{a \in \mathbb{F}_{p^m} / g(a) = 0\} &= \# \{a \in \mathbb{F}_{p^m} / a^{p^n} = a\} \\ &= \# \{a \in \mathbb{F}_{p^m}^* / a^{p^n - 1} = 1\} + 1 \end{aligned}$$

Comme  $n|m \Rightarrow p^n - 1 | p^m - 1$ , donc  $\# \{a \in \mathbb{F}_{p^m}^* / a^{p^n - 1} = 1\} = \underbrace{p^n - 1}_{\text{cyclique}}$

d'où

$$\# \{a \in \mathbb{F}_{p^m} / g(a) = 0\} = p^n$$

ce qui prouve que  $g$  possède toutes ses racines dans  $\mathbb{F}_{p^m}$ .  $\mathbb{F}_{p^m}$  est un corps de décomposition de  $g$ . D'après le théorème (\*2),  $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^n} \hookrightarrow \mathbb{F}_{p^m}$

ce qui prouve que  $\mathbb{F}_{p^n} \hookrightarrow \mathbb{F}_{p^m}$ .

d'où le théorème:

Th

$$\mathbb{F}_{p^n} \hookrightarrow \mathbb{F}_{p^m} \iff n|m$$

$$K = \mathbb{F}_{p^a} \hookrightarrow \mathbb{F}_{p^{an}} = L \quad \text{ou} \quad [L; \mathbb{F}_{p^a}] = n$$

D'après le a) et le b)  $\exists f$  irréductible de degré  $n$  sur  $\mathbb{F}_{p^a}[X] = K[X]$

(5)

Remarque: exo

$\forall x \neq 0$  [2] et [5]  $\exists n$  tel que  $x | \underbrace{99 \dots 9}_{n \text{ neuf}}$ .

c'est une conséquence de l'exercice (5).

$p$  premier  $\text{car}(\mathbb{F}_q) = p \quad q = p^m$

$\Delta(n, p) = 1 \quad K = \text{csp des racines de } X^n - 1 \in \mathbb{F}_q[X]$

a)  $\underline{n \mid (\#K - 1)}$

$$\{x \in K / x^n = 1\} \subset K^*$$

$\{x \in K / x^n = 1\}$  est un sous-groupe du groupe multiplicatif  $(K^*, \times)$

Cherchons  $\# \{x \in K / x^n = 1\}$ . Tous les éléments de  $\{x \in K / x^n = 1\}$  sont distincts car le polynôme  $X^n - 1$  admet pour dérivée  $nX^{n-1}$  et  $nx^{n-1} \neq 0$  (1)  
 $\forall x \in \{x \in K / x^n = 1\}$

(1) comporte un piège  $nx^{n-1} \neq 0$  car  $\Delta(n, p) = 1$ , donc  $nx^{n-1} = 0 \Rightarrow n = 0$   
 et  $0 \notin \{x \in K / x^n = 1\}$ .

On a montré que  $\# \{x \in K / x^n = 1\} = n$

Le théorème de Lagrange permet de conclure :

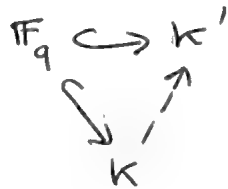
$$n \mid \underbrace{\#K - 1}_{\#K^*}$$

CQFD

b) Soit  $m'$  tel que  $n \mid q^{m'} - 1$

Prenons  $q = p^\alpha$   $q^{m'} = p^{\alpha m'}$

$\exists K'$  de cardinal  $\#K' = p^{\alpha m'}$  et tel que  $\mathbb{F}_q \hookrightarrow K'$  (car  $\alpha \mid \alpha m'$ )



Problème :  $f = X^n - 1$  se décompose dans  $K' \Rightarrow K' =$  corps de décomposition  
 et donc  $K' \hookrightarrow K$

$$\Downarrow$$

$$q^{m'} = (q^m)^\beta \text{ i.e. } m\beta = m'$$

$n \mid q^{m'} - 1 \Rightarrow n \mid \#K'^*$  et  $(K'^*, x)$  est cyclique (sous-groupe mult.

d'un corps fini)  $\Rightarrow \exists ! G$  sous-groupe de  $(K'^*, x)$

$$\Rightarrow G = \{x \in K'^* / x^n = 1\} \text{ et } \#G = n$$

Donc  $K' =$  corps de décomposition de  $f$ .

CQFD

$$\exists \underline{p \in \mathcal{P}}: \begin{cases} \alpha \in \mathbb{N}^* \\ n \in \mathbb{N}^* \end{cases} \quad \Delta(n, p) = 1$$

$$\text{Alors } \exists m \in \mathbb{N}^* / n \mid p^{\alpha m} - 1$$

On utilise le a) et le b)

$$q = p^\alpha \quad \mathbb{F}_q \quad \beta = X^n - 1 \quad \left\{ \begin{array}{l} \exists m \\ \mathbb{F}_q \hookrightarrow \mathbb{F}_{q^m} \text{ et } n \mid q^m - 1 \end{array} \right.$$

c-à-d  $n \mid p^{\alpha m} - 1$

● Si p n'est pas premier :

$$p = \prod_{\alpha_i > 0} p_i^{\alpha_i}$$

$$\exists m_i \quad n \mid p_i^{\alpha_i m_i} - 1$$

$$\text{Prends } m = \text{ppcm } m_i \quad n \mid p_i^{\alpha_i m} - 1$$

$$p_i^{\alpha_i m} \equiv 1 \pmod{n}$$

$\Downarrow$

$$\prod p_i^{\alpha_i m} \equiv 1 \pmod{n}$$

QFD

Remarque : 1) Si  $\Delta(n, 10) = 1$ ,  $\exists m$  tel que  $n \mid \underbrace{9 \dots 9}_{m \text{ fois } 9}$  (P)

(Branche  $p=10$  et  $\alpha=1$ )

2) Façon élémentaire de montrer (P)

$$\frac{a}{b} = x + \frac{10^q y}{b} \quad \text{et} \quad \exists i / 10^{i+1} y - \overline{z} = y \quad \text{ou} \quad \frac{10^4 y}{b} = c_0 \dots c_1 c_0 c_1 \dots$$

(Rappel :  $\forall h \mid \alpha \in \mathbb{R}$ ;  $\alpha \in \mathbb{Q} \Leftrightarrow$  l'écriture décimale de  $\alpha$  est périodique)  
à partir d'un certain rang.



$$\text{d'où } (10^{l+1}-1)\alpha = 3\beta$$

$$\text{si } y = \frac{\alpha}{\beta} \quad \sigma(\alpha, \beta) = 1$$

Preons  $\alpha = 1$ .

$$(n, 10) = 1$$

$$\frac{1}{n} = \underbrace{N_1 \cdot 10^{-p}}_{\text{partie non périodique}} + 10^{-p} x \quad \text{où } x \text{ est périodique} \quad (1)$$

$$\left| \begin{array}{l} x = 0, \underbrace{c_0 \dots c_i c_0 \dots c_i \dots}_{N_2} \\ \text{est donc tel que } N_2 \\ 10^q x - N_2 = x \quad (q \in \mathbb{N}) \end{array} \right.$$

$$10^q - N_2 = x \Rightarrow \frac{N_2}{10^q - 1} = x \quad (2)$$

$$(1) \text{ et } (2) \Rightarrow 10^p (10^q - 1) = N n$$

$$\sigma(10^p, n) = 1 \Rightarrow n \mid 10^q - 1$$

Exercice 1

$K$  = corps fini de cardinal  $q$  impair

a) Montrer que  $1 \neq -1$     b)  $\varphi: K^* \rightarrow K^*$  est un morphisme de groupes de noyau  $\text{Ker } \varphi = \{ \pm 1 \}$ .

En déduire que  $H = \{x^2 / x \in K^*\}$  possède  $\frac{q-1}{2}$  éléments, et que  $\# K^* / H = 2$

c) Critère d'Euler

$x \in K^*$   
( $q$  impair)

$$x^{\frac{q-1}{2}} = \begin{cases} 1 & \text{si } x \in H \\ -1 & \text{sinon.} \end{cases}$$

(Ind: th. Fondamental,  $K^*$  est cyclique, et  $G \subset K^* \# G = d \Leftrightarrow G = \{x \in K^* / x^d = 1\}$ )

d) Application :  $\exists a \in \mathbb{Z}/p\mathbb{Z}$  ( $p \in \mathcal{P}$ )  $a^2 = -1 \Leftrightarrow p \equiv 1 \pmod{4}$

Polynômes cyclotomiques :

• Soit  $n \geq 1$  ( $n \in \mathbb{N}$ )

•  $\Phi_n$  = polynôme cyclotomique d'indice  $n$  si :

$$\Phi_n(X) = \prod_{\omega(\xi_i)=n} (X - \xi_i)$$

$\omega(\xi) = n \Leftrightarrow \xi$  élément d'ordre  $n$  de  $\mathbb{C}^*$   
où  ~~$n$  est inf~~ (et  $\xi$  racine primitive  $n$ -ième de l'unité)

Gnà:  $\deg \Phi_n = \varphi(n)$

Gn pose  $\Phi_1(X) = X - 1$

Calculer  $\Phi_{12} = X^4 - X^2 - 1$

Calculer  $\Phi_p(X)$  où  $p \in \mathcal{P}$ .

$$\Phi_p(X) = 1 + \dots + X^{p-1}$$

Pro1 |  $\Phi_n$  est un polynôme à coefficients entiers.  
c.à.d  $\Phi_n \in \mathbb{Z}[X]$

Pro2 | On a :  $\forall n \in \mathbb{N}$   

$$X^n - 1 = \prod_{d|n} \Phi_d$$

Preuve Pro2:

$$G_d = \{ \zeta \in \Gamma_n / \omega(\zeta) = d \} \quad \text{ou} \quad \Gamma_n = \{ \zeta \in \mathbb{C}^* / \zeta^n = 1 \}$$

$$\text{Il est clair que } \Gamma_n = \bigsqcup_{d|n} G_d \Rightarrow X^n - 1 = \prod_{\zeta \in \Gamma_n} (X - \zeta)$$

$$X^n - 1 = \prod_{d|n} \prod_{\zeta \in G_d} (X - \zeta) = \prod_{d|n} \Phi_d$$

(Note : on retrouve la formule d'Euler  $\phi(n) = \sum_{d|n} \mu(d)$ )

Preuve Pro1:

$$\Phi_n = \frac{X^n - 1}{\prod_{\substack{d|n \\ d < n}} \Phi_d}$$

Réurrence : (H) Supposons que  $\Phi_m \in \mathbb{Z}[X] \quad \forall m < n$

On est dans la situation suivante  $P = \frac{Q}{R}$   $\left. \begin{array}{l} R \text{ monique} \\ Q, R \in \mathbb{Z}[X] \\ P \in \mathbb{C}[X] \end{array} \right\} \Rightarrow P \in \mathbb{Z}[X]$

En effet  $PR = Q \Rightarrow$  le coefficient de plus haut degré de  $P$  est entier.

$$\begin{array}{l} \text{cof.} \quad a \quad b \quad c \\ \quad \quad P \quad R = Q \\ \text{deg} \quad p \quad n \end{array} \left\{ \begin{array}{l} a_p \in \mathbb{Z} \\ a_{p-1} ? \end{array} \right. \quad \underbrace{c_{p+n-1}}_{\in \mathbb{Z}} = \underbrace{a_p}_{\in \mathbb{Z}} \underbrace{b_{n-1}}_{\in \mathbb{Z}} + a_{p-1} \underbrace{b_n}_{=1} \Rightarrow a_{p-1} \in \mathbb{Z} \text{ c.q.f.d.}$$

②  $f(X) = X^4 - 2X^2 + 9 \in \mathbb{Q}[X]$

Corps des racines de  $f$  ?

$$\begin{aligned} f(X) &= X^4 - 6X^2 + 9 + 4X^2 \\ &= (X^2 - 3)^2 + 4X^2 = (X^2 - 3 - 2iX)(X^2 - 3 + 2iX) \end{aligned}$$

$$\Delta' = -1 + 3 = 2$$

donc les racines  $\left\{ \begin{array}{l} i \pm \sqrt{2} \\ -i \pm \sqrt{2} \end{array} \right.$

Le corps des racines de  $f$  sur  $\mathbb{Q}$  est  $\mathbb{Q}(i, \sqrt{2})$

$$[\mathbb{Q}(i, \sqrt{2}) ; \mathbb{Q}] = \underbrace{[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}(\sqrt{2})]}_{\text{pol. min. } X^2+1} \times \underbrace{[\mathbb{Q}(\sqrt{2}) ; \mathbb{Q}]}_{2, \text{ pol. min. } X^2-2}$$

2°  $f(X)$  est irréductible sur  $\mathbb{Q}$ .

On a  $f(i + \sqrt{2}) = 0$ .

Quel est le degré de  $i + \sqrt{2}$  sur  $\mathbb{Q}$  ? (1, 2, 3 ou 4.)

(critère d'Eisenstein servirait pour le pentiel)

- $i + \sqrt{2}$  n'est pas de degré 1,
- $i + \sqrt{2}$  n'est pas de degré 3,  $\exists g / g(i + \sqrt{2}) = 0$  et  $f = gh$

Il serait de degré 1 et  $f$  admettrait une racine rationnelle, ce qui n'est pas, puisque ses racines sont  $i \pm \sqrt{2}$  et  $-i \pm \sqrt{2}$ .

- Si  $i + \sqrt{2}$  était de degré 2, on aurait

$$\exists g \pm X^2 + aX + b \quad / \quad -1 + 2 + 2i\sqrt{2} + ai + a\sqrt{2} + b = 0$$

$\Downarrow$

$$2\sqrt{2} + a = 0 \quad a \in \mathbb{Q}$$

impossible.

- Donc  $i + \sqrt{2}$  est de degré 4, et par suite  $f$  est irréductible sur  $\mathbb{Q}$ .

QPF)

Groupe de galois de  $f(X) = X^4 - 2X^2 + 9$

On sait que  $\text{gal}(\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}) \cong \text{gal}_{\mathbb{Q}}(f) \hookrightarrow S_4$   
4 éléments (car  $f$  est séparable)

En effet :  $\text{gal}_{\mathbb{Q}}(f) \hookrightarrow S_{\{x_1, x_2, x_3, x_4\}}$  morphisme injectif  
 $\theta \mapsto \theta|_{\{x_1, x_2, x_3, x_4\}}$

Comme  $f$  est séparable  $\# \text{gal}_{\mathbb{Q}}(f) = [\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = 4$

Un groupe de cardinal 4 est commutatif (les ordres des éléments ne pouvant être que 1, 2 ou 4)

Donc  $\text{gal}_{\mathbb{Q}}(f)$  est isomorphe à un groupe  $\mathbb{Z}/4\mathbb{Z}$  ou  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Soit  $\theta \in \text{gal}_{\mathbb{Q}}(f) : i^2 = -1 \Rightarrow \theta(i) = \pm i$

$$(\sqrt{2})^2 = 2 \Rightarrow \theta(\sqrt{2}) = \pm \sqrt{2}$$

$$\text{donc } \theta^2(i) = i \quad (\text{car } \theta^2 = \theta \circ \theta)$$
$$\theta^2(\sqrt{2}) = \sqrt{2}$$

Donc  $\theta^2 = \text{Id}$ .

Tout élément de  $\text{gal}_{\mathbb{Q}}(f)$  est d'ordre 2. C'est le groupe de Klein.

$$\text{gal}_{\mathbb{Q}}(f) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Service de renseignement Thér

SDECE

Indication : Tous les exos du Mac-Lane

p 301 (> partie du sujet)

(~ p 3299)  
298

③ Sur  $P \in F[X]$  irréductible

$$\left. \begin{array}{l} \deg P = q \\ \Delta([K:F], q) = 1 \end{array} \right\} \Rightarrow P \text{ irréductible sur } K$$

important

On peut écrire :

$$P = f \cdot g \quad \text{sur } K \quad \left| \begin{array}{l} f \text{ irréductible sur } K \text{ et } \deg f = n \\ f, g \in K[X] \end{array} \right.$$

$$\begin{array}{c} \bullet \quad \left[ \begin{array}{ccc} F & \rightarrow & K \rightarrow K[X]_{(f)} = L \\ & \searrow & \nearrow \\ & F[X]_{(P)} & \end{array} \right] \quad \begin{array}{l} (f) \\ (P) \end{array} \quad \begin{array}{l} \text{(corps de rupture de } f) \\ \text{(corps de rupture de } P) \end{array} \quad \begin{array}{l} [L:K] = n \\ \text{(le corps de rupture s'injecte} \\ \text{dans tout corps de} \end{array} \end{array}$$

$$[L:F] = \cancel{q} [K:F] \times n \quad (1)$$

$\Rightarrow$  car  $L$  possède au moins une racine de  $P$ .

$$\begin{aligned} (1) \Rightarrow [L:F] &= n [K:F] \\ &= q [L:F[X]_{(P)}] \end{aligned}$$

$$\text{d'où } n [K:F] = q [L:F[X]_{(P)}]$$

$$\Downarrow \text{ (Gauss) }$$

$$q \mid n$$

$$\text{Mais } n \leq q, \text{ donc } \boxed{q = n}$$

$$\text{Donc } \boxed{P = f \text{ irréductible sur } K.}$$

$\text{CQFD}$

Tests

④ Irréductible ou non ?

$X^2 + 3$  sur  $\mathbb{Q}(\sqrt{7})$  oui

$X^2 + 1$  sur  $\mathbb{Q}(i\sqrt{2})$  ~~oui~~ car  $i = a + bi\sqrt{2}$   $a, b \in \mathbb{Q}$

$X^3 + 8X - 2$  sur  $\mathbb{Q}(\sqrt{2})$

On peut utiliser l'exercice ③ :

⊗  $f \in F[X]$  irréductible  
 $F$  CK de degré premier  
avec  $\deg f$  }  $\Rightarrow f$  premier sur  $F$

⊗ Si ce polynôme avait une racine dans ce corps, son corps de rupture s'injecterait dans  $\mathbb{Q}(\sqrt{2})$ .

$X^3 + 8X - 2$  est irréductible sur  $\mathbb{Q}$ . Son corps de rupture est de degré 3, et ne peut s'injecter dans  $\mathbb{Q}(\sqrt{2})$  de degré 2 sur  $\mathbb{Q}$ . Donc  $X^3 + 8X - 2$  est irréductible sur  $\mathbb{Q}(\sqrt{2})$ .

⊗ Faire  $(a + b\sqrt{2}) = X$  dans  $X^3 + 8X - 2$  et trouver que ce n'est pas possible ( $a, b \in \mathbb{Q}$ ). Comme  $X^3 + 8X - 2$  est de degré 3,  $X^3 + 8X - 2$  irréductible sur  $\mathbb{Q} \Leftrightarrow$  pas de racines dans  $\mathbb{Q}$ .

$f = X^5 + 3X^2 - 9X - 6$  sur  $\mathbb{Q}(\sqrt{7}, \sqrt{5}, 1+i)$

⊗  $[\mathbb{Q}(\sqrt{7}, \sqrt{5}, 1+i) : \mathbb{Q}] = 8 = 2 \times 2 \times 2$

(car  $(1+i)^2 - 1 = -1 \Rightarrow [\mathbb{Q}(1+i) : \mathbb{Q}] = 2$ )

D'après l'exercice ③,  $\deg f = 5$  et  $\gcd(5, 8) = 1 \Rightarrow f$  est irréductible sur  $\mathbb{Q}(\sqrt{7}, \sqrt{5}, 1+i)$

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{7}) \subset \mathbb{Q}(\sqrt{7}, \sqrt{5}) \subset \mathbb{Q}(\sqrt{7}, \sqrt{5}, 1+i)$$

$\begin{matrix} 2 & & 2 & & 2 \\ X^2-5 & & & & X^2+1 \end{matrix}$

**Tests** (5)  $f \in \mathbb{Q}[x]$  (~~corps  $K$  donné~~): Donner  $[K : \mathbb{Q}]$   
corps des racines  $\mathbb{Q}$  de  $f = K$

a)  $\beta = X^3 - X^2 - X - 2$

est racine évidente  $B = (X-2) \underbrace{(X^2 + X + 1)}_{j, j^2}$

$$K = \mathbb{Q}(j) \text{ de degré } 2 \text{ sur } \mathbb{Q}$$

$$b) \underline{x^3 - 2 = 0} \quad \sqrt[2]{e} \quad j\sqrt[3]{2} \quad j^2\sqrt[3]{2}$$

$\mathbb{Q}(j, \sqrt[3]{2})$  de degré 6 sur  $\mathbb{Q}$ .

can  $\mathbb{Q} \subset \mathbb{Q}(j) \subset \mathbb{Q}(j, \sqrt[3]{2})$  (conempile)

$$c) \underline{x^4 - 7 = 0} \quad \left\{ \begin{array}{l} \pm \sqrt[4]{7} \\ \pm i \sqrt[4]{7} \end{array} \right.$$

$$K = \mathbb{Q}(i, \sqrt[4]{7}) \text{ de degré } 8 \text{ sur } \mathbb{Q}$$

$$d) \underline{(x^2 - 2)(x^2 - 5)}$$

$$K = \mathbb{Q}(\sqrt{2}, \sqrt{5}) = \text{degré } 2 \times 2 = 4$$



## Equation du 3<sup>e</sup> degré

Soit  $k$  un corps de caractéristique  $\neq 2$  et  $\neq 3$ . Soit  $f = X^3 + pX + q$  irréductible de  $k[X]$ . Soit  $k(x_1, x_2, x_3) = K$  le corps des racines de  $X^3 + pX + q$ .

$$\text{On a } f(X) = \prod_{i=1}^3 (X - x_i).$$

$$\text{Soit } \Delta = \prod_{i < j} (x_i - x_j). \text{ On pose } D \doteq \text{Discr}(f) = \Delta^2$$

$$\text{On note } G = \text{Gal}_k(f) \hookrightarrow \mathcal{I}_{\{x_1, x_2, x_3\}} = \mathcal{I}_3$$

Les racines  $x_1, x_2, x_3$  sont distinctes car  $f$  irréductible et  $k$  de car.  $\neq 3 \Rightarrow f$  séparable.

$$\text{Soit } \sigma \in G, \sigma(\Delta) = \varepsilon_\sigma \Delta \Rightarrow \sigma(D) = D \Rightarrow \underline{D \in k} \\ (\text{cf } k = (k(f))^G)$$

$$H = \{\theta \in G \mid \theta(\Delta) = \Delta\} = k(\Delta)^G \subset \mathcal{A}_3 \text{ (permutations paires)}$$

Les sous-groupes de  $\mathcal{A}_3$  sont:  $\mathcal{A}_3$  et  $\{\text{Id}\}$ , donc  $H = \mathcal{A}_3$  ou  $H = \{\text{Id}\}$

$$\text{Si } H = \{\text{Id}\}, \text{ alors } \#G = 2 \neq [K:k] \geq \underbrace{[k[X]_{(f)} : k]}_{\text{deg du corps de rupture}} = 3$$

(car il n'y a pas d'autres sous-groupes d'ordre 3 que  $\mathcal{A}_3 = \{1, (123), (213)\}$ )

$$\text{Donc } H = \mathcal{A}_3.$$

$$\text{Ainsi } G = \mathcal{I}_3 \text{ ou } \mathcal{A}_3.$$

1° Si  $G = \mathcal{I}_3$ ,  $\exists \theta \in G \mid \theta(\Delta) = -\Delta \Rightarrow \boxed{\Delta \notin k}$  si le corps est de caractéristique 2,  $-\Delta = \Delta$  et cette implication est fausse.

2° Si  $G = \mathcal{A}_3$ ,  $\forall \theta \in G; \theta(\Delta) = \Delta \Rightarrow \boxed{\Delta \in k}$

La structure du groupe de Galois est donc parfaitement déterminée par  $\Delta$ , suivant que  $\Delta \in$  ou  $\notin k$ .

Pb: Calculer D

$$f(x) = \prod_i (x - x_i)$$

$$f'(x) = (x - x_1)(x - x_2) + (x - x_2)(x - x_3) + (x - x_3)(x - x_1)$$

$$f'(x_1) f'(x_2) f'(x_3) = -(x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2 = -D$$

$$-D = (3x_1^2 + p)(3x_2^2 + p)(3x_3^2 + p)$$

$$\text{Mais } x_i^2 = -p \mp \frac{q}{x_i} \Rightarrow 3x_i^2 + p = -2p \mp \frac{3q}{x_i}$$

d'où :

$$D = \left( \frac{3q}{x_1} + 2p \right) \left( \frac{3q}{x_2} + 2p \right) \left( \frac{3q}{x_3} + 2p \right)$$

$$D = \frac{27q^3}{x_1 x_2 x_3} + \underbrace{18q^2 p \left( \frac{1}{x_1 x_2} + \frac{1}{x_2 x_3} + \frac{1}{x_3 x_1} \right)}_{\substack{0 \text{ car } x_1 + x_2 + x_3 = 0}} + 12p^2 q \left( \frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} \right) + 8p^3$$

$$0 \text{ car } x_1 + x_2 + x_3 = 0$$

$$D = -27q^2 + \frac{12p^2 q}{-1} + 8p^3$$

$$D = -27q^2 - 4p^3$$

$$\boxed{D = -4p^3 - 27q^2}$$

$$X^3 + pX + q$$

$$\begin{cases} D \text{ carré dans } \mathbb{Q} \Leftrightarrow \text{gal}_{\mathbb{Q}}(f) = \mathcal{A}_3 \\ D \neq \text{carré dans } \mathbb{Q} \Leftrightarrow \text{gal}_{\mathbb{Q}}(f) = \mathcal{S}_3 \end{cases}$$

Application :

$$\bullet X^3 + 2X + 1 \in \mathbb{Q}[X]$$

$$D = +32 - 27 = 5$$

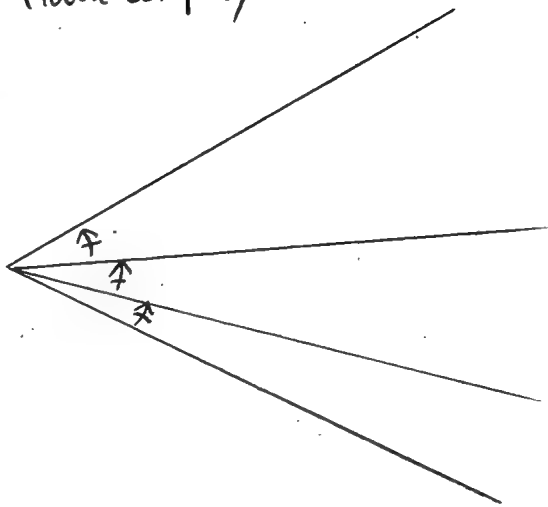
$$\Delta^2 = D \Rightarrow \Delta \not\in \mathbb{Q} \text{ donc } \underbrace{\Delta}_{\sqrt{5}} \text{ donc } \boxed{G = \mathcal{S}_3}$$

$$\bullet X^3 - 3X + 1$$

$$D = 81 \text{ donc } G = \mathcal{A}_3 \quad \text{cf. } \neq$$

# Trisection de l'angle (rien compris)

Tracer les trisectrices d'un angle à la règle et au compas.



On ne peut résoudre à la règle et au compas que les équations de degré  $2^n$ .

$$\cos 3\theta = 4\left(\cos^3 \theta - \frac{3}{4} \cos \theta\right) = 4\cos^3 \theta - 3\cos \theta$$

Pour  $\theta = \frac{\pi}{3}$ ,  $\cos \theta$  est de degré 3 car  $4X^3 - 3X + 1 = 0$  est irréductible sur  $\mathbb{Q}$ .

$$X^3 - 3X + 1 = 0$$

$$(*) \quad X = u+v \quad X^3 - 3X + 1 = u^3 + v^3 + (u+v)(\underbrace{3uv - 3}_{=1}) + 1 = 0$$

$$\begin{cases} u^3 + v^3 = -1 \\ uv = 1 \end{cases}$$

On pose  $U = u^3 \quad V = v^3$

$$\begin{cases} U + V = -1 \\ UV = 1 \end{cases}$$

$$T^2 + T + 1 = 0$$

$$\begin{cases} U = j \\ V = j^2 \end{cases}$$

$$\begin{cases} U = e^{i\frac{2\pi}{3}} \\ V = e^{-i\frac{2\pi}{3}} \end{cases}$$

Les racines de l'équation  $X^3 - 3X + 1 = 0$  sont

$$1) \quad u = e^{i\frac{2\pi}{9}} \quad v = e^{-i\frac{2\pi}{9}} \quad u+v = 2\cos\frac{2\pi}{9}$$

$$2) \quad ju + j^2v = 2\cos\frac{8\pi}{9}$$

$$3) \quad j^2u + jv = 2\cos\frac{4\pi}{9}$$

On a  $\cos 2x = 2\cos^2 x - 1$ , donc  $L = \text{corps des rac. de } X^3 - 3X + 1$

$L = \mathbb{Q}\left(\cos\frac{2\pi}{9}\right)$   $\cos\frac{2\pi}{9}$  de polynôme minimal de  $X^3 - 3X + 1 = 0$   $\Rightarrow \text{Gal}(L/\mathbb{Q}) = \mathbb{Z}/3\mathbb{Z}$

## Propriété universelle du corps de rupture

Th |  $f$  polynôme irréductible  $k \subset K = \text{corps de rupture de } f$

Def |  $\forall k \rightarrow L$  tel que  $\exists x \in L / f(x) = 0$

Alors  $\exists \varphi: k \hookrightarrow L$  morphisme qui rend le diagramme suivant commutatif:

$$\begin{array}{ccc} & k & \\ \alpha \swarrow & & \searrow \beta \\ & k \xrightarrow{\varphi} L & \\ & (\beta = \varphi \circ \alpha) & \end{array}$$

c'est une définition possible du corps de rupture de  $f$ .

Th |  $\forall f$  polynôme,  $k \subset K = \text{corps des racines de } f$

$\forall k \rightarrow L / f = a \prod (x - x_i) \quad x_i \in L$

$\exists \varphi: k \hookrightarrow L$  morphisme qui rend le diagramme

$$\begin{array}{ccc} & k & \\ \swarrow & & \searrow \\ & k \rightarrow L & \end{array}$$

## Rappel:

A anneau principal (par définition: intègre et tout idéal est principal)

On a pas de mal à définir la divisibilité:

$$a, b \in A \quad a|b \Leftrightarrow \exists c \in A / b = ac$$

Notons  $U = \{x \in A / \exists y \in A \quad xy = 1\}$ . On remarque que  $\forall a \in A \quad \forall u \in U \quad u|a$  et  $ua|a$

$(U, \cdot) = \text{groupe pour la multiplication}$ .

Def: On dit que  $a \in A \setminus U$ ,  $a \neq 0$  est irréductible si les seuls diviseurs de  $a$  sont les diviseurs obligatoires, c.à.d.  $u \in U$  ou  $ua$ .

Def:  $a$  et  $b$  sont premiers entre eux si ils n'ont pas d'autre diviseur commun que  $u \in U$ .

Le côté PGCD - PPCM se fait bien.

Si  $D$  est un carré dans  $\mathbb{Q}$

$$(\Delta) \quad (x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2 = a^2 \quad a \in \mathbb{Q}$$

$\Uparrow$

$$(x_1 - x_2)(x_1 - x_3)(x_2 - x_3) = \pm a \quad (1)$$

$$x_3 = -x_1 - x_2 \quad (\text{valeur somme des racines de } \underbrace{x^3 + px + q}_= P)$$

$$(1) \text{ donne : } (x_1 - x_2)(2x_1 + x_2)(x_1 + 2x_2) = a$$

$$[\mathbb{Q}(x_1) : \mathbb{Q}] = 3 \quad \text{car } P \text{ est irréductible}$$

$$(x_1 - X)(2x_1 + X)(x_1 + 2X) - a \in \mathbb{Q}(x_1)$$

et une racine de ce polynôme est  $x_2$

$$l = [\underbrace{\mathbb{Q}(x_1, x_2)} : \mathbb{Q}(x_1)] \leq 3$$

c'est le corps des racines  
de  $P$

$$l = 1, 2 \text{ ou } 3.$$

• Si  $l = 3$ , le corps des racines de  $P$  aurait pour degré  $3 \times 3 = 9$ .

Ce n'est pas possible car  $\deg[\mathbb{Q}(x_1, x_2) : \mathbb{Q}] \leq 3!$

• Si  $l = 2 \Rightarrow \exists$  diviseur de degré 1.

## Corps de rupture d'un polynôme irréductible sur $k[X]$ : $P \in k[X]$ .

Définition: Soit  $P \in k[X]$  un polynôme irréductible sur  $k[X]$ . On appelle corps de rupture de  $P$  tout sur-corps  $R$  de  $k$  qui vérifie:

1)  $\exists x \in R / P(x) = 0$

2)  $\forall K$  corps  $k \subset K / \exists x \in K P(x) = 0$ , alors  $R \subset K$

On dira que  $R$  est un plus petit corps, à isomorphisme près, contenant au moins une racine de  $P \in k[X]$ .

Pro 1:  $k \subset \mathbb{K}[X]_{(P)}$  et  $\exists \xi \in \mathbb{K}[X]_{(P)} / P(\xi) = 0$ .

Pro 2:  $\forall K / \exists x \in K P(x) = 0$  alors  $\mathbb{K}[X]_{(P)} \subset K$   
et  $k \subset K$

Pro 3: Les corps de rupture sont uniques, à isomorphisme (de corps) près.

Provenons les 3 propositions:

Pro 1 On considère  $\pi: k[X] \rightarrow \mathbb{K}[X]_{(P)}$  et  $\pi|_k = \text{id}$

$$Q \mapsto \bar{Q}$$

$$\forall a, b \in k \quad \bar{a} = \bar{b} \Leftrightarrow \overline{a-b} = \bar{0} \Leftrightarrow P \mid a-b \Rightarrow a-b=0 \text{ (cf. P. ir.)} \\ \Rightarrow a=b.$$

$\pi|_k = \text{id}$  est donc injective. C'est un morphisme de corps. Donc  $k \subset \mathbb{K}[X]_{(P)}$

Mentions l'existence de  $\xi / P(\xi) = 0$ :

$$\xi = \bar{X} \quad P(\bar{X}) = \overline{P(X)} = \bar{0} \quad \text{oui}$$

Pro 2

$k \subset K$  donc  $\exists \Phi$  maph. inj.  $k \xrightarrow{\Phi} K$

$$\begin{array}{ccc} & & \uparrow \\ & \downarrow & \nearrow \\ & \mathbb{K}[X]_{(P)} & \xrightarrow{\tilde{\Phi}} \end{array}$$

$$\begin{cases} \tilde{\Phi}(a) = \Phi(a) & a \in k \\ \tilde{\Phi}(X) = x \in K \\ \text{(où } x / P(x) = 0 \text{)} \end{cases}$$

$\tilde{\Phi}$  ainsi définie ne dépend pas du représentant choisi ?

Si  $\tilde{f} = \tilde{g}$  où  $f, g \in k[X]$ , on a :

$$\begin{cases} \tilde{\Phi}(f) = \Phi(f)(\alpha) & (\text{où } f = \sum_{i=0}^n a_i X^i \Rightarrow \Phi(f) = \sum_{i=0}^n \Phi(a_i) X^i \in K[X]) \\ \tilde{\Phi}(g) = \Phi(g)(\alpha) \end{cases}$$

$$\tilde{f} = \tilde{g} \Leftrightarrow f - g \text{ divisible par } P \Leftrightarrow f - g = PQ \quad P, Q \in k[X]$$

$$\text{d'où } \tilde{\Phi}(f) - \tilde{\Phi}(g) = (\Phi(f) - \Phi(g))(\alpha) = \Phi(f - g)(\alpha) = \Phi(PQ)(\alpha)$$

$$\begin{aligned} \tilde{\Phi}(f) - \tilde{\Phi}(g) &= \underbrace{\Phi(P)(\alpha)}_{=0} \cdot \Phi(Q)(\alpha) = 0 \quad \text{car} \\ &= 0 \quad (\text{car } P(\alpha) = 0) \end{aligned}$$

**Pro 3** Unicité des corps de rupture :

$R, R'$  deux corps de rupture de  $P \in k[X]$

Par définition :

$$\begin{array}{ccc} k & \hookrightarrow & R' \\ & \searrow \varphi_1 & \nearrow \\ & R & \end{array} \quad \begin{array}{l} \text{car } R \text{ est de rupture} \\ \text{et } \exists \alpha \in R' / P(\alpha) = 0 \end{array}$$

$$\begin{array}{ccc} k & \hookrightarrow & R \\ & \searrow \varphi_2 & \nearrow \\ & R' & \end{array} \quad \begin{array}{l} (\varphi_i = \text{maph. inj. de corps}) \\ \text{car } R' \text{ est de rupture} \\ \text{et } \exists \alpha \in R / P(\alpha) = 0 \end{array}$$

Prendons  $R = k[X]_{(P)}$  corps de rupture trouvé grâce aux Pro 1 et 2.

$$\dim_R R = \deg P < \infty \text{ donc}$$

$$\begin{cases} k[X]_{(P)} \xrightarrow{\varphi_1} R' & (1) \quad \varphi_1 \text{ inj} \Rightarrow \dim_R R \leq \dim_R R' \\ R' \xrightarrow{\varphi_2} k[X]_{(P)} & \varphi_2 \text{ injective} \Rightarrow \dim_R R' \leq \dim_R R < \infty \end{cases} \quad (2)$$

(1) donner alors :  $\dim_R R = \dim_R R' \Rightarrow \varphi_1 \text{ inj. est aussi surj} \Rightarrow \varphi_1 \text{ est 1 isomorphisme d'ev.}$   
 (2) CQFD

## Théorème Important

$k \subset K$  et  $P \in k[X]$  irréductible sur  $k$ .

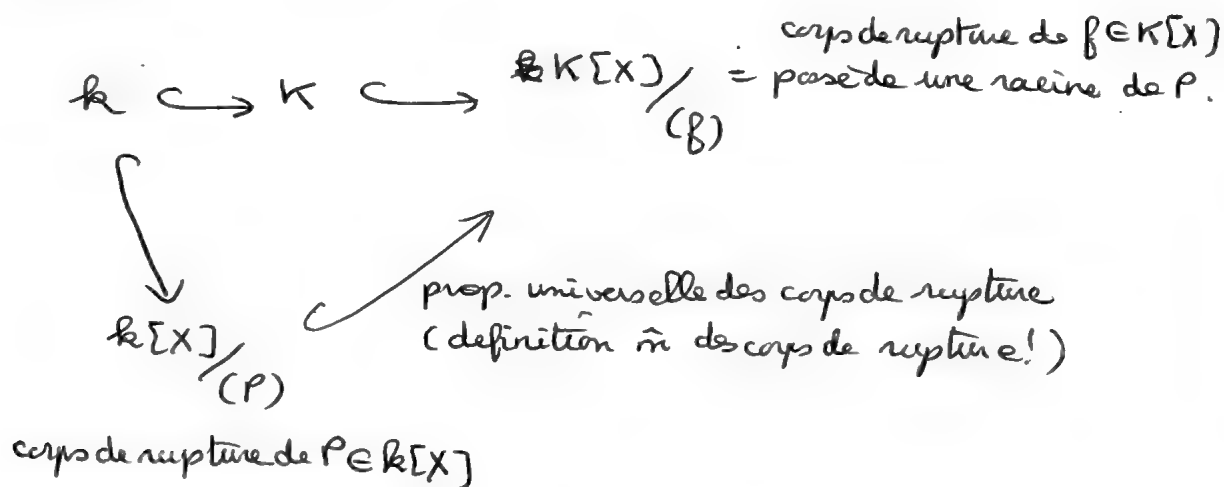
Alors :  $\Delta([K:k]; \deg P) = 1 \Rightarrow P$  irréductible sur  $K$

démonstration :

$P \neq \text{cte}$  car  $P$  ir. sur  $k$

Donc  $\exists \beta$  irréductible sur  $K$  /  $P = \beta \gamma$   $\beta, \gamma \in K[X]$

On a le diagramme :



$$[K[X]/(\beta) : k] = (\deg \beta) [K : k] = [K[X]/(\beta) : k[X]/(P)] \cdot \deg P$$

et (th. Gauss)  $\deg P \mid \deg \beta$  or  $\deg \beta \leq \deg P \Rightarrow \deg \beta = \deg P$

et  $P = \text{cte} \cdot \beta$  où  $\text{cte} \in K$   
 $\text{cte} \neq 0$

Q.E.D.



$\text{Gal}_F(P)$ ? où  $\begin{cases} F = \mathbb{Q}(\zeta) \text{ et } \zeta = \text{racine } 5\text{-ième primitive de l'unité.} \\ P = X^5 - 7 \end{cases}$

Préparable. Notons  $L = \text{corps des racines de } P = \mathbb{Q}(\zeta, \alpha) = F(\alpha)$

$$\# \text{Gal}_F(P) = [L : F] = [F(\alpha) : F]$$

Trouver un polynôme minimal de  $\alpha$  sur  $F$ .

$X^5 - 7$  est irréductible sur  $\mathbb{Q}$ .

l'est-il sur  $F = \mathbb{Q}(\zeta)$ ?  $[F : \mathbb{Q}] = 4$  et  $\deg P = 5$  premiers entre eux.

$$\text{d'où } [F(\alpha) : F] = 5 \Rightarrow \# \text{Gal}_F(P) = 5$$

Mais  $\text{Gal}_F(P) \subset \mathcal{I}_5$   $\# \mathcal{I}_5 = 5!$  éléments.

les racines de  $P = X^5 - 7$  sont  $\{\alpha, \zeta\alpha, \zeta^2\alpha, \zeta^3\alpha, \zeta^4\alpha\}$  tous distincts.

Soit  $\sigma \in \text{Gal}_F(P)$  défini par  $\begin{cases} \sigma(\alpha) = \zeta\alpha \\ \sigma(\zeta) = \zeta \text{ car } \zeta \in F \end{cases}$

On a  ~~$\sigma(\alpha) = \zeta\alpha$~~

	$\alpha$	$\zeta\alpha$	$\zeta^2\alpha$	$\zeta^3\alpha$	$\zeta^4\alpha$
$\sigma()$	$\zeta\alpha$	$\zeta^2\alpha$	$\zeta^3\alpha$	$\zeta^4\alpha$	$\alpha$

$$\text{et } \sigma^2(\alpha) = \sigma(\zeta\alpha) = \zeta^2\alpha$$

$$\sigma^3(\alpha) = \zeta^3\alpha$$

$$\sigma^4(\alpha) = \zeta^4\alpha$$

$$\sigma^5(\alpha) = \alpha$$

$$\Rightarrow \sigma^5 = \text{Id.}$$

$$\Rightarrow \omega(\sigma) = 5$$

$$(\sigma^k \neq \text{Id si } k < 5)$$

Soit donc générateur de  $\text{Gal}_F(P) \simeq \mathbb{Z}/5\mathbb{Z}$

Avant

$F_n$  irréductible. (voir cours p 4.181)

lemme:  $P$  irréductible sur  $k$ . Soit  $K$  une extension de  $k$ :

$$\Delta([K : k], \deg P) = 1 \Rightarrow P \text{ irréductible sur } K.$$

	$\alpha$	$\sigma \alpha$	$\sigma^2 \alpha$	$\sigma^3 \alpha$	$\sigma^4 \alpha$	
$S_1$	$\sigma \alpha$	$\sigma^2 \alpha$	$\sigma^3 \alpha$	$\sigma^4 \alpha$	$\alpha$	associé à (12345)
$S_2$	$\sigma^2 \alpha$	$\sigma^3 \alpha$	$\sigma^4 \alpha$	$\alpha$	$\sigma \alpha$	associé à (13524)
$S_3$	$\sigma^3 \alpha$	$\sigma^4 \alpha$	$\alpha$	$\sigma \alpha$	$\sigma^2 \alpha$	associé à (14253)
$S_4$	$\sigma^4 \alpha$	$\alpha$	$\sigma \alpha$	$\sigma^2 \alpha$	$\sigma^3 \alpha$	associé à (15432)
$S_5$	$\alpha$	$\sigma \alpha$	$\sigma^2 \alpha$	$\sigma^3 \alpha$	$\sigma^4 \alpha$	associé à (1)

Preuve du lemme: Montrer que

$$K \subset K$$

$P \in K[x]$  irréductible sur  $K$ .

$$\Delta([K:K]; \deg P) = 1 \Rightarrow P \text{ irréductible sur } K$$

(oui)

- \* ① a) Deux ensembles  $E$  et  $F$  sont dits équipotents, s'il existe une bijection  $f: E \rightarrow F$ .  
Montrer que l'équipotence est une "relation d'équivalence".  
On note  $\#E$  ou  $\text{card } E$  la "classe d'équivalence de  $E$ ".  
b) On note  $\text{card } E \leq \text{card } F$ , s'il existe une injection  $f: E \rightarrow F$ .

Montrer que  $\begin{cases} \text{card } E \leq \text{card } F \\ \text{card } F \leq \text{card } E \end{cases} \Rightarrow \text{card } E = \text{card } F$

(théorème de Bernstein.)

Indication:  $f: E \rightarrow F$  et  $g: F \rightarrow E$  étant des injections  
construire  $\varphi: E \rightarrow F$  bijectif de façon que:  
 $\varphi = f$  sur  $(g \circ f)^n[E - g(F)]$   
 $\varphi = g^{-1}$  sur  $(g \circ f)^n[g(F) - f(E)]$   $n \in \mathbb{N}$

c)  $\leq$  est une relation d'ordre

- ② a) On appelle groupe cyclique un groupe engendré par un élément. Montrer qu'il est isomorphe à  $\mathbb{Z}$  ou  $\mathbb{Z}/n\mathbb{Z}$ .  
b) Soit  $x \in G$ ,  $G$  cyclique d'ordre  $n$ ,  $x$  générateur:  
 $x^k$  engendre  $G \Leftrightarrow k$  et  $n$  premiers entre eux.  
c) Si  $G$  et  $H$  sont cycliques d'ordre  $m, n$ :  
 $G \times H$  est cyclique si &  $m, n$  sont premiers entre eux.  
d)  $G$  fini,  $\#G = p$  premier  $\Rightarrow G$  est cyclique.

③ Groupe diédral.

Soit  $\sigma, \tau \in S_n$  définis par

$$\tau(i) = i+1, \text{ si } 1 \leq i \leq n-1, \tau(n) = 1$$

$$\sigma(i) = n-i+1, i = 1, \dots, n$$

- a) Montrer que  $\sigma^2 = 1$   $\tau^n = 1$   
 $\tau \circ \sigma \circ \tau = \sigma$

b) en théorie que  $s, r$  engendrent sans  $\sigma_n$  un sous groupe à  $2n$  éléments :

$$\Delta_n = \{ Id, r, r^2, \dots, r^{n-1}, \sigma, \sigma \circ r, \dots, \sigma \circ r^{n-1} \}$$

c) Montrer que  $\Delta_n$  s'identifie aux ~~paramètres~~  
~~l'un des~~ isométries d'un polygone régulier  
à  $n$  côtés.

d) Déterminer les sous groupes de  $A_n$ , les sous groupes distingués.

VAMPIRE

(4) On appelle sous groupe dérivé de  $G$ , noté  $DG$  le sous groupe engendré par les  $x y x^{-1} y^{-1}$

a) montrer que  $D(G)$  est un sous groupe distingué  
et que  $H \triangleleft G$  :

~~$G/H$  commutatif  $\iff H \supset DG$~~

b) on note  $D^2(G) = D(D(G))$ , ...,  $D^n(G) = D(D^{n-1}(G))$

Montrer que les conditions suivantes sont équivalentes

(4)  $\exists r$   $D^{r+1}(G) = \{e\}$  e element neutre de  $G$ .

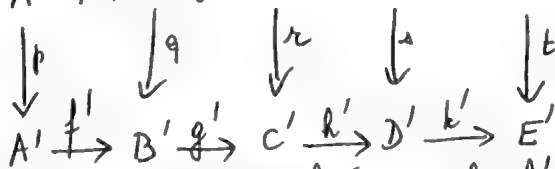
(ii) Il existe des sous-groupes  $H_i$  :  $\{e\} = H_0 \subset H_1 \subset \dots \subset H_n = G$

tel que :  $H_i \triangleleft H_{i+1}$  et  $H_{i+1}/H_i$  commutatif.

(ii) ~~et en plus~~  $H_i \triangleleft G$

x (5) ("l'homme des cinq")

Soit  $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D \xrightarrow{k} E$  un diagramme



im Diagramme

Le groupe commutatif (i.e.  $g \circ f = f' \circ g$  etc...) à lignes exactes

Alors: a)  $p$  surjectif,  $q$ ,  $s$  injectifs  $\Rightarrow r$  injectif

b)  $q, s$  surjectifs,  $t$  injectif  $\Rightarrow r$  surjectif

c) umkehrf. (a)+(b)  $\Rightarrow$  1 bijektiv

intéret : " si  $p, q, r \in E$   
sont des isomorphismes de groupes,  
alors  $r$  est un isomorphisme  
de groupes".

$E$  muni d'une relation d'ordre  $\leq$ .

Ordre total :  $\forall x, y \in E \quad x \leq y \text{ ou } y \leq x$

Bon ordre : Quel que soit  $A \subseteq E, A \neq \emptyset \quad \exists x_0 \in A$  tel que  
 $x_0 = \inf \{y / y \in A\}$   
 (c.-à.-d.  $x_0 = \min A$ )

1)  $E$  bien ordonné  $\Rightarrow E$  totalement ordonné.  $\mathbb{N}; \mathbb{N} \cup \{\omega\}; \{0; \dots; n\} = S_n$

2) Donner des exemples d'ensembles bien ordonnés  $\mathbb{R}; \mathbb{Z}$   
 " " " totalement ordonnés et non bien ordonnés.

3)  $\mathbb{N} \times \mathbb{N} \quad (a, b) \leq (a', b') \Leftrightarrow a < a' \text{ ou } \{a = a' \text{ et } b \leq b'\}$

Montrer que l'ordre lexicographique sur  $\mathbb{N} \times \mathbb{N}$  est une relation de bon ordre.

4) Tout ensemble bien ordonné admet un plus petit élément.

$E$  bien ordonné  $\begin{cases} \text{(i) } \forall x \in E \quad \exists y \doteq x+1 / x < y \text{ et } \forall z > x \quad z \geq y \\ \text{ou} & \text{(successeur de } x) \\ \text{(ii) } \forall y \in E \quad y \leq x \end{cases} \quad \text{on note } y = x'$

Solutions :

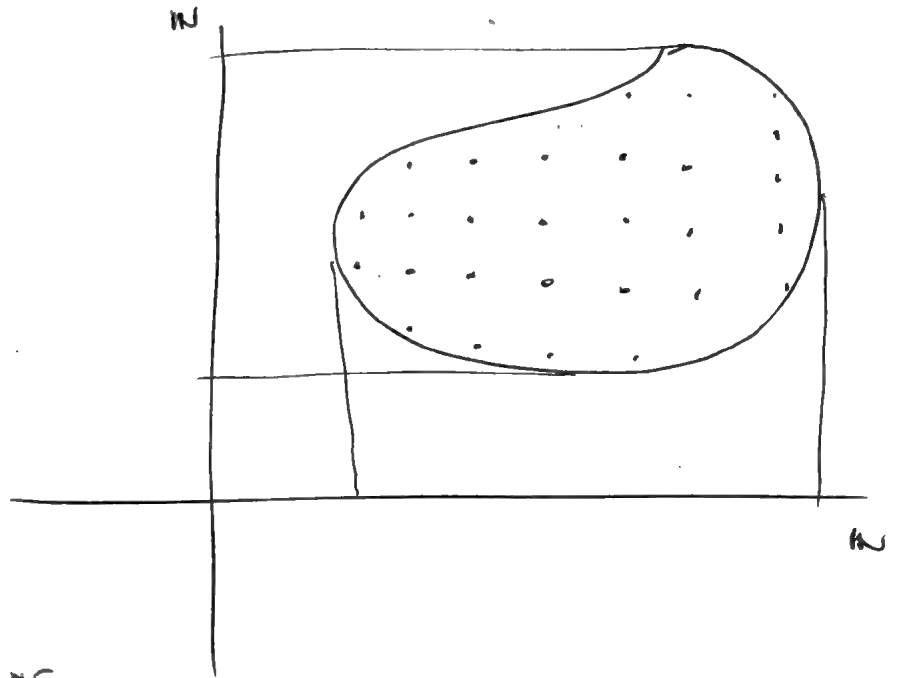
Preuve de 1)  $\inf \{x, y\} = z \in \{x, y\} \Rightarrow z = x \text{ ou } z = y$

Notations :  $S_x = \{y / y < x\} \quad \bar{S}_x = \{y / y \leq x\}$

a)  $x' = \min (E \setminus \bar{S}_x)$  où  $E = \bar{S}_x$

3)

Soit  $A \subset \mathbb{N} \times \mathbb{N}$   $A \neq \emptyset$



Soit  $p_1 : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$   
 $(a, b) \mapsto a$

$p_1(A) \subset \mathbb{N}$  et  $p_1(A) \neq \emptyset$

Donc  $\inf p_1(A) = a_0$

Considérons :

$\{b / (a_0, b) \in A\} \neq \emptyset$

$b_0 = \min \{b / (a_0, b) \in A\} \in \mathbb{N}$

Alors  $(a_0, b_0)$  convient :  $(a_0, b_0) = \min \{(a, b) / (a, b) \in A\}$

En effet :  $\forall (a_0, b_0) \in A$

$\forall (a, b) \in A$

$(a_0, b_0) \leq (a, b)$

naïve  
 $a_0 \leq a$

si  $a_0 < a$  fini.

si  $a_0 = a$   $b_0 \leq b$   
 est c'est encore  
 vrai

Remarque 1 : On aurait pu prendre n'importe quel ensemble  $E$  bien ordonné à la place de  $\mathbb{N}$ .

Remarque 2 :  $\forall x \in E$  où  $E$  est bien ordonné,  $S_x$  est bien ordonné.

Ordre inverse :  $(E, \leq)$ , l'ordre inverse de  $E$  est défini par :

$$x < y \Leftrightarrow y \leq x$$

Soit  $(E, \leq)$  un bon ordre et  $E \neq \emptyset$

$(E, \leq)$  et  $(E, <)$  sont bien ordonnés  $\Leftrightarrow E$  fini

preuve :

$(\Rightarrow)$  Soit  $x_0 = \inf E$   $A = \{x_0, x_0+1, \dots, x_0+n, \dots\} \subset E$

où  $x_0+(n+1) = \text{successeur de } x_0+n$ .

Il existe  $p / x_0+p = \sup A$  donc  $A = \{x_0, \dots, x_0+p\}$  (1)

Soit  $y \in E$  . Si  $y > x_0+p$  alors  $x_0+(p+1)$  existerait

car  $\{y \in E / y > x_0 + p\} \neq \emptyset$ . Mais alors,  $x_0 + p$  ne serait pas le plus grand élément de  $A$ , ce qui contredit (1)

• Donc  $x_0 \leq y \leq x_0 + p$

Soit  $\{k / x_0 + k \leq y\} \neq \emptyset$ . Posons  $\sup \{k / x_0 + k \leq y\} = k_0$

1<sup>er</sup> cas  $k_0 < p$   $x_0 + k_0 \leq y < x_0 + k_0 + 1$

Et forcément  $y = x_0 + k_0$  (sinon, on contredirait le fait que  $x_0 + k_0 + 1$  soit le successeur de  $x_0 + k_0$ )

Ainsi  $y \in A$ .

2<sup>nd</sup> cas  $k_0 = p$   $x_0 + p \leq y \leq x_0 + p \Rightarrow y = x_0 + p \in A$

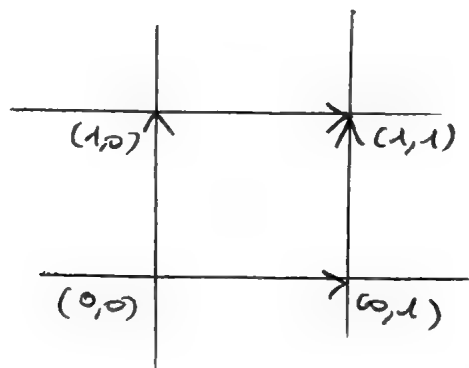
• D'où  $E = A$  est fini.

( $\Leftarrow$ ) évident, puisque  $(E, \leq)$  est bien ordonné et  $E$  fini.



$A \times B$   $A, B$  ordonnés

L'ordre produit sur  $A \times B$  :  $(a, b) \leq (a', b') \Leftrightarrow \begin{cases} a \leq a' \\ \text{et} \\ b \leq b' \end{cases}$



les éléments  $(1,0)$  et  $(0,1)$  ne sont pas comparables.

$\{0,1\} \times \{0,1\}$  n'est pas totalement ordonné.

Remarque : Deuxième démonstration

Posons  $V = \{x / S_x \text{ est fini}\}$  et  $y_0 = \sup V$ . Montrer que  $E = S_{y_0} \cup \{y_0\}$

Th (lemme) |  $E$  ensemble,  $\mathcal{G} \subset \mathcal{P}(E)$  ( $\mathcal{G} = \text{Sgothique}$ )  
 $\mathcal{G} \xrightarrow{p} E \quad p(X) \notin X$   
 Alors il existe  $M \notin \mathcal{G}$  muni d'un bon ordre tel que  
 $\forall x \in M \quad \begin{cases} S_x \in \mathcal{G} \\ p(S_x) = x \end{cases} \quad \text{où } S_x = (\leftarrow, x[$

Remarque : 1)  $E \notin \mathcal{G}$

2) Si  $\emptyset \notin \mathcal{G}$ , alors  $M = \emptyset$  convient.

Si  $M$  convient et  $M \neq \emptyset$ ,  $x_0 = \min M$  et  $S_{x_0} = \emptyset \in \mathcal{G}$  impossible.

Donc si  $\emptyset \notin \mathcal{G}$ ,  $M = \emptyset$  convient et c'est le seul qui convienne !

cas I :  $E$  est fini On suppose désormais que  $\emptyset \in \mathcal{G}$ .

(Si  $M$  existe, soit  $x_0 = \min M \Rightarrow p(x_0) = p(S_{x_0}) = p(\emptyset)$ )  
 Posons donc  $x_0 = p(\emptyset)$ .

Si  $\{x_0\} \notin \mathcal{G}$ , on prend  $M = \{x_0\}$

Sinon  $\{x_0\} \in \mathcal{G}$ , on prend  $x_1 = p(\{x_0\})$

Supposons définis par récurrence  $x_0, \dots, x_n$  tels que  $\{x_0, \dots, x_n\} \in \mathcal{G}$

pour  $i \leq n-1$  et  $x_{i+1} = p(\{x_0, \dots, x_i\})$

2 cas : \*  $\{x_0, \dots, x_n\}$  convient

ou \*  $\{x_0, \dots, x_n\} \in \mathcal{G}$  et l'on définit  $x_{n+1} = p(\{x_0, \dots, x_n\})$

Si  $E$  est fini, l'opération s'arrête nécessairement.

Remarque : Si l'opération ne s'arrête pas, ~~soit~~ :

$A = \{\underbrace{x_0, \dots, x_n}_{\text{suite bien ordonnée (infinie)}}\}$  | si  $A \notin \mathcal{G}$  et  $A$  est fini  
 | sinon  $p(\{x_0, \dots, x_n, \dots\}) = x_0$

d'où  $\downarrow$   
 $\{x_0, x_1, \dots, x_n, \dots\}$   
 $\{x_0, \dots\}$



Cas général

$E$  ensemble  $\mathcal{G} \subset \mathcal{P}(E)$

$p: \mathcal{G} \rightarrow E \quad p(x) \notin X$

$\exists H$  bien ordonné

1)  $H \notin \mathcal{G}$

2)  $\forall x \in H \quad \begin{cases} S_x \in \mathcal{G} \text{ où } S_x = (\leftarrow, x[ \\ p(S_x) = x \end{cases}$

$x \in \mathcal{G}$

$x$  si  $\emptyset \in \mathcal{G}$  alors  $H = \emptyset$  convient.

$x \notin \mathcal{G}$

Soit  $\mathcal{M} \subset \mathcal{P}(E)$  défini par  $U \in \mathcal{M} \Leftrightarrow U$  bien ordonné et  $\forall x \in U \quad S_{U,x} \in \mathcal{G} \text{ et } p(S_{U,x}) = x$

Alors  $M = \bigcup_{U \in \mathcal{M}} U$  répondra à la question.

$U, U' \in \mathcal{M}$ , soit  $V \subset U \cap U'$

• premier élément de  $U$  ou de  $U'$  :  $\pi_0 = p(\emptyset)$

•  $V = \{x \in U \cap U' \mid S_{U,x} = S_{U',x} \text{ et l'ordre induit par } U \text{ et } U' \text{ est le même}\}$

• Si  $U \setminus V \neq \emptyset$  et si  $U' \setminus V \neq \emptyset$  on pose  $\begin{cases} \pi = \text{Min}_U(U \setminus V) \Rightarrow S_{U,\pi} = V \\ \pi' = \text{Min}_{U'}(U' \setminus V) \Rightarrow S_{U',\pi'} = V \end{cases}$

Donc  $V \in \mathcal{G}$  et  $p(V) = \pi = \pi' \Rightarrow \pi \in V$  impossible

Donc  $U \setminus V = \emptyset$  ou  $U' \setminus V = \emptyset \Leftrightarrow V = U$  ou  $V = U' \Leftrightarrow U \subset U'$  ou  $U' \subset U$

On pose alors  $M = \bigcup_{U \in \mathcal{M}} U$

$\begin{cases} x \in M \\ y \in M \end{cases} \Rightarrow \exists U \in \mathcal{M} \mid \begin{cases} x \in U \\ y \in U \end{cases}$

$x \leq y$  dans  $M \Leftrightarrow x \leq y$  dans  $U$   $x$  ne dépend pas de  $U$  car

$$\left| \begin{array}{l} x \in U \subset U' \\ y \in U \subset U' \end{array} \right. \Rightarrow \text{l'ordre } x \leq y \text{ dans } U \Leftrightarrow x \leq y \text{ dans } U'$$

\* M est bien ordonné.

(NB: Si  $x \in U$  et si  $y \in M / y \leq_U x$  alors  $y \in U$ )

~~Remarquons que  $x \in U$   $y \leq_M x$  alors  $y \in U$~~

$$\emptyset \neq A \subset M \quad x \in A \quad \exists U \in \mathcal{M} / x \in U \text{ et } A \cap U \neq \emptyset$$

$$y \leq x \Rightarrow y \in U$$

$U$  est bien ordonné et  $A \cap U \neq \emptyset \Rightarrow \exists x_0 = \min_U (A \cap U)$

Alors  $x_0 = \min_M A : y \in A \text{ et } y \leq x_0 \Rightarrow y \in U \Rightarrow y \in A \cap U$

$\Rightarrow y = x_0$  et  $x_0 \in A$

donc  $x_0 = \text{élément minimal de } A$   
dans  $A$  (bien ordonné) et  $x_0 \in A$

$\Downarrow$

$$x_0 = \min A$$

$$* \quad \underline{S_{M,x} = S_{U,x}} \quad (\text{si } x \in U)$$

\*  $M \notin \mathcal{G}$  Si  $M \in \mathcal{G}$   $p(M) = a \notin M$  et  $M \cup \{a\} \in \mathcal{M}$

Mais alors  $M \cup \{a\}$  est aussi un ensemble bien ordonné,  $\text{car } p(M) = p(S_a) = a \in M$

ce qui est absurde puisque  $M = \bigcup_{U \in \mathcal{M}} U$

### Théorème de Zermelo.

Tout ensemble  $E$  peut être bien ordonné.

preuve:

$$\mathcal{G} = \mathcal{P}(E) \setminus \{E\}$$

$$p : \mathcal{G} \rightarrow E$$

$$X \mapsto x_X \in E \setminus X \quad \text{car } E \setminus X \neq \emptyset$$

(C)

# [ (Axiome du choix)

$(X_i)_{i \in I}$  famille d'ensemble indexée par  $I$ .

$$\forall i \in I \quad X_i \neq \emptyset \iff \prod_{i \in I} X_i \neq \emptyset$$

La ligne (C) montre le choix d'un élément du produit  $\prod_{x \in G} (E \setminus x)$

D'après le lemme (si dur à montrer)

$\exists H \subseteq E$  bien ordonné tel que  $H \notin G \Rightarrow H = E$  bien ordonné.

Remarque: L'axiome du choix est équivalent au théorème de Zorn.

## Théorème de Zorn

Tout ensemble adonné inductif admet un élément maximal

$(E, \leq)$  est dit inductif si  $F \subseteq E$  F totalement ordonné  $\Rightarrow F$  possède un majorant.

On montre le théorème suivant, plus fort que le théorème de Zorn:

Th  $\left\{ \begin{array}{l} \text{Tout ensemble dans lequel les parties bien ordonnées} \\ \text{majorées admet un élément maximal.} \end{array} \right.$

$G \subseteq \mathcal{P}(E)$  tel que  $G = \{ A \in \mathcal{P}(E) \mid A \text{ bien ordonné et } \exists m_A \text{ majorant strict de } A \}$

$$p: G \rightarrow E$$

$A \mapsto p(A)$  majorant strict de  $A$

$\exists M$  bien ordonné /  $\forall x \in M \quad s_x \in M$  et  $p(s_x) = x$   
et  $M \notin G$

(\*) Si l'ordre sur  $M$  est l'ordre induit par l'ordre sur  $E$ . Alors  $M$  est une partie bien ordonnée de  $E$ , donc  $M$  admet un majorant. et  $M \neq \emptyset \Rightarrow m \in M$ .

Donc  $m$  = élément maximal de  $M$

(\*) [ Montrons (\*) que  $y \leq_M x \Rightarrow y \leq_E x$

$$\begin{array}{c} \Downarrow \\ y \in S_x \quad x = p(S_x) = \text{majorant au sens de } E \\ \Downarrow \\ y \leq_E x \end{array}$$

Inversement, si  $y \leq_E x$ , on a  $y \leq_M x$  ou  $x \leq_M y$ . Le cas ou  $x \leq_M y$  est exclus par le sens direct. Donc  $y \leq_M x$ .

Ainsi  $y \leq_M x \Leftrightarrow y \leq_E x$

□ CQFD

Base d'un espace vectoriel

Soit  $E$  un e.v.  $\{x_i\}_{i \in I} \subset E$

Définition: Une famille d'éléments de  $E$  est linéairement indépendante (ou "libre") si

$$\forall J \subset I \quad \text{fini} \quad \sum_{i \in J} \lambda_i x_i = 0 \Rightarrow \forall i \in J \quad \lambda_i = 0$$

Définition: Une famille  $\{x_i\}_{i \in I} \subset E$  est une base si

c'est

1) une famille libre

2) génératrice de  $E$  (c.à.d.  $\forall x \in E \exists J \text{ fini}$

$$\exists \lambda_i / x = \sum_{i \in J} \lambda_i x_i)$$

(C'est la définition algébrique des bases)

Alas, avec ces définitions :

- ① Les familles libres forment un système inductif pour  $C$
- ② libre + maximale  $\Rightarrow$  génératrice.

- ①  $\mathcal{G}' =$  ensemble de familles <sup>libres</sup>  $F$  telle que
- $$\forall F, F' \in \mathcal{G}' \quad F \subset F' \text{ ou } F' \subset F$$

Soit  $G = \bigcup_{F \in \mathcal{G}'} F$ . Montrons que  $G$  est une famille libre :

$$\forall \{x_1, \dots, x_n\} \subset G \text{ fini} \quad \sum_{i=1}^n \lambda_i x_i = 0$$

$$\forall i \quad \exists F_i \quad x_i \in F_i$$

On peut supposer que  $F_1 \subset \dots \subset F_n$ , d'où  $x_i \in F_n \quad \forall i \in [1, n]$

Mais  $\sum_{i=1}^n \lambda_i x_i = 0$  est une relation ne faisant intervenir que des vecteurs de  $F_n$ , donc  $\lambda_i = 0 \quad \forall i$ .

Donc  $G$  est une famille libre. D'évidence  $G \supset F \quad \forall F \in \mathcal{G}'$

Soit  $B$  une partie libre maximale.

- ② Soit  $x \in E$ .
- \* Si  $x \in B \quad x = 1 \cdot x$
  - \*  $x \notin B \quad B \cup \{x\}$  non libre.

$$\text{Donc } \exists x_1, \dots, x_n \in B \quad \exists \lambda_i \quad \lambda_1 x_1 + \dots + \lambda_n x_n + \lambda x = 0$$

$$\text{avec } (\lambda_1, \dots, \lambda) = (0, \dots, 0). \text{ Alas } \lambda \neq 0 \text{ et } x = -\frac{\lambda_1}{\lambda} x_1 - \dots - \frac{\lambda_n}{\lambda} x_n$$

$$\text{et } x \in \langle B \rangle \text{ (engendré par les } B)$$

Donc  $B$  est une base.

## Exercices :

①  $A$  anneau commutatif unitaire. Montrer, en utilisant le théorème de Zorn, que l'ensemble des idéaux propres de  $A$  est inductif. Montrer que pour tout idéal  $I \subsetneq A$ , il existe  $M$  maximal tel que  $I \subsetneq M \subsetneq A$ .

② Posons  $\mathbb{N}^{(\mathbb{N})} = \{ (n_1, n_2, \dots, n_p, \dots) \mid n_i \in \mathbb{N}; \exists p_0, n_p = 0 \text{ pour } p \geq p_0 \}$

$\mathbb{N}^{(\mathbb{N})}$  est dénombrable. Je le munis de l'ordre lexicographique  $\leq$ .  
~~Montrer qu'il~~ <sup>est</sup> est bien ordonné pour  $\leq$ .

Cependant, l'ordre lexicographique n'est pas un bon ordre sur  $\mathbb{N}$ .

## Solutions :

①  $(A, +, \times, e)$

Soit  $\mathcal{I}$  l'ensemble des idéaux propres de  $A$ .

1° est inductif : Soit  $\mathcal{F}$  une famille totalement ordonnée pour l' $\subset$ .

Alors  $\bigcup_{I \in \mathcal{F}} I \in \mathcal{I}$  est un majorant de  $\mathcal{F}$ , dans  $\mathcal{I}$ .

Montrons que  $\bigcup_{I \in \mathcal{F}} I \in \mathcal{I}$  :  $\bigcup_{I \in \mathcal{F}} I$  est bien un sous-groupe additif de  $(A, +)$  en vertu de l'hypothèse "totalement ordonnée" pour  $\mathcal{F}$ . Le fait que  $\bigcup_{I \in \mathcal{F}} I$  soit un idéal est alors évident :

$$\forall x \in A \quad \forall y \in \bigcup_{I \in \mathcal{F}} I \quad \exists I \in \mathcal{F} / y \in I \text{ et alors } xy \in I \subset \bigcup_{I \in \mathcal{F}} I$$

Le théorème de Zorn s'applique donc à  $\mathcal{I}$  :  $\mathcal{I}$  possède un élément maximal. Enonçons le résultat :

"Tout anneau commutatif unitaire possède au moins un idéal maximal".

2° Soit  $I$  un idéal de  $A$ . Soit  $\mathcal{J}_I = \{J \text{ idéal de } A / J \neq A \text{ et } J \supset I\}$   
 $\mathcal{J}_I$  est non vide car  $I \in \mathcal{J}_I$ . On montre, de la même manière qu'en 1°, que  $\mathcal{J}_I$  est un ensemble inductif pour  $\subset$ . Le théorème de Zorn nous indique que'il existe  $M \in \mathcal{J}_I$  maximal.

$M$  est donc un idéal, maximal dans  $\mathcal{J}_I$ .

$\forall F$  idéal propre de  $I$  tel que  $F \supset M$  alors  $F \supset I \Rightarrow F \in \mathcal{J}_I$   
 et  $F \supset M \Rightarrow F = M$ , ce qui montre que  $M$  est aussi un idéal maximal dans l'ensemble  $\mathcal{I}$  des idéaux propres de  $A$ .

Enonçons le résultat :

" Soit  $I$  un idéal de  $A$ . Il existe un idéal maximal  $M$   
 tel que  $I \subset M$ ."

②  $\mathbb{N}^{(\mathbb{N})}$  est dénombrable comme réunion dénombrable d'ensembles dénombrables.

Ni  $\mathbb{N}^{(\mathbb{N})}$ , ni  $\mathbb{N}^{\mathbb{N}}$  ne sont bien ordonnés pour l'ordre lexicographique.

En effet : soit  $A = \{x_p = (0, 0, \dots, 0, 1, 0, \dots) / p \in \mathbb{N}^*\} \subset \mathbb{N}^{(\mathbb{N})} \subset \mathbb{N}^{\mathbb{N}}$

Lemme : Si  $n \leq x_p$  alors  $n_1 = \dots = n_{p-1} = 0$  ( $p \geq 2$ )

(où  $n = (n_1, \dots)$ )

Le seul minorant de  $A$  possible est  $0 = (0, \dots)$

Si  $\mathbb{N}^{(\mathbb{N})}$  était bien ordonné, la partie non vide  $A \subset \mathbb{N}^{(\mathbb{N})}$  admettrait un minimum, et ce ne peut être que  $0$ . Mais  $0 \notin A$ . Donc  $\mathbb{N}^{(\mathbb{N})}$  n'est pas bien ordonné.

Construisons un bon ordre sur  $\mathbb{N}^{(\mathbb{N})}$  : Pour tout  $p$ , on a une injection

$$\begin{array}{ccc} \mathbb{N}^p & \xrightarrow{\varphi_p} & \mathbb{N}^{(\mathbb{N})} \\ & \varphi_p & \\ (a_1, \dots, a_p) & \longmapsto & (a_1, \dots, a_p, 0, \dots) \end{array}$$

On a

$$\varphi_p(\mathbb{N}^p) \subset \varphi_{p+1}(\mathbb{N}^{p+1})$$

$$\varphi_{p+1}(\mathbb{N}^p \times \{0\})$$

et :  $\mathbb{N}^{(\mathbb{N})} = \bigcup_{p \in \mathbb{N}^*} \mathbb{N}^p$

$$\begin{cases} a = (a_1, \dots, a_p, \dots) \\ b = (b_1, \dots, b_p, \dots) \end{cases} \quad a \neq b$$

Je dis que :  $a < b \iff \left\{ \exists p \in \mathbb{N}^* / \begin{cases} 1) a_i = b_i \quad i > p \\ 2) a_p < b_p \end{cases} \right\}$

En d'autres termes,  $a_p < b_p$  où  $p = \sup \{k / a_k \neq b_k\}$ . Ce sup existe car  $\{k / a_k \neq b_k\}$  est forcément fini.  $\blacksquare$

1°/  $(\mathbb{N}^{(\mathbb{N})}, \leq)$  induit sur  $\varphi_p(\mathbb{N}^p)$  l'ordre "anti-lexicographique"

$$\left. \begin{array}{l} 2^\circ / \text{ Si } (\underline{a}) \notin \varphi_p(\mathbb{N}^p) \\ (\underline{b}) \in \varphi_p(\mathbb{N}^p) \end{array} \right\} \Rightarrow (\underline{b}) < (\underline{a})$$

$$3^\circ / \exists p, A \cap \varphi_p(\mathbb{N}^p) \neq \emptyset \quad \text{Min}(A \cap \varphi_p(\mathbb{N}^p))$$

$$4^\circ / \text{ successeur de } \varphi_p(\mathbb{N}^p) : e_{p+1}$$



Remarque :

lemme:  $(E_n)$  dénombrable  $\Rightarrow \bigcup_{n \in \mathbb{N}} E_n$  est dénombrable.

preuve 1:

$a_{n,p}$   $p$ -élément de  $E_n$

$F_k = \{ a_{n,p} / n+p = k \}$  est fini (possède  $k+1$  éléments)

D'où  $E = \bigcup_{k \in \mathbb{N}} F_k$

preuve 2:  $(a_1, \dots, a_p) \rightarrow (a_1, \dots, a_p, 0, \dots) = (\underline{a})$

•  $F'_k = \{ (\underline{a}) \mid a_1 + \dots + a_p \leq k \}$  et  $p \leq k$

•  $F'_k$  est fini et  $\mathbb{N}^{(p)} = \bigcup_{k \in \mathbb{N}} F'_k$

•  $(F'_k)$  sont emboîtées:  $F'_k \subset F'_{k+1}$

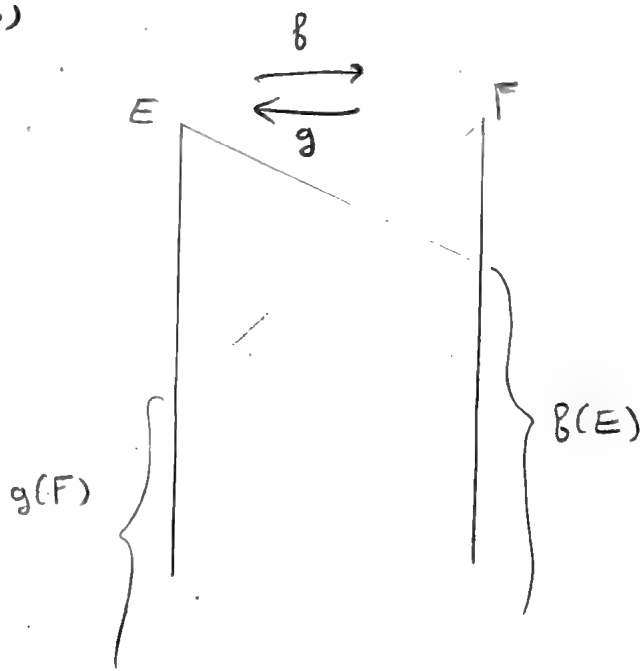
TDALG 1 (feuille TD)

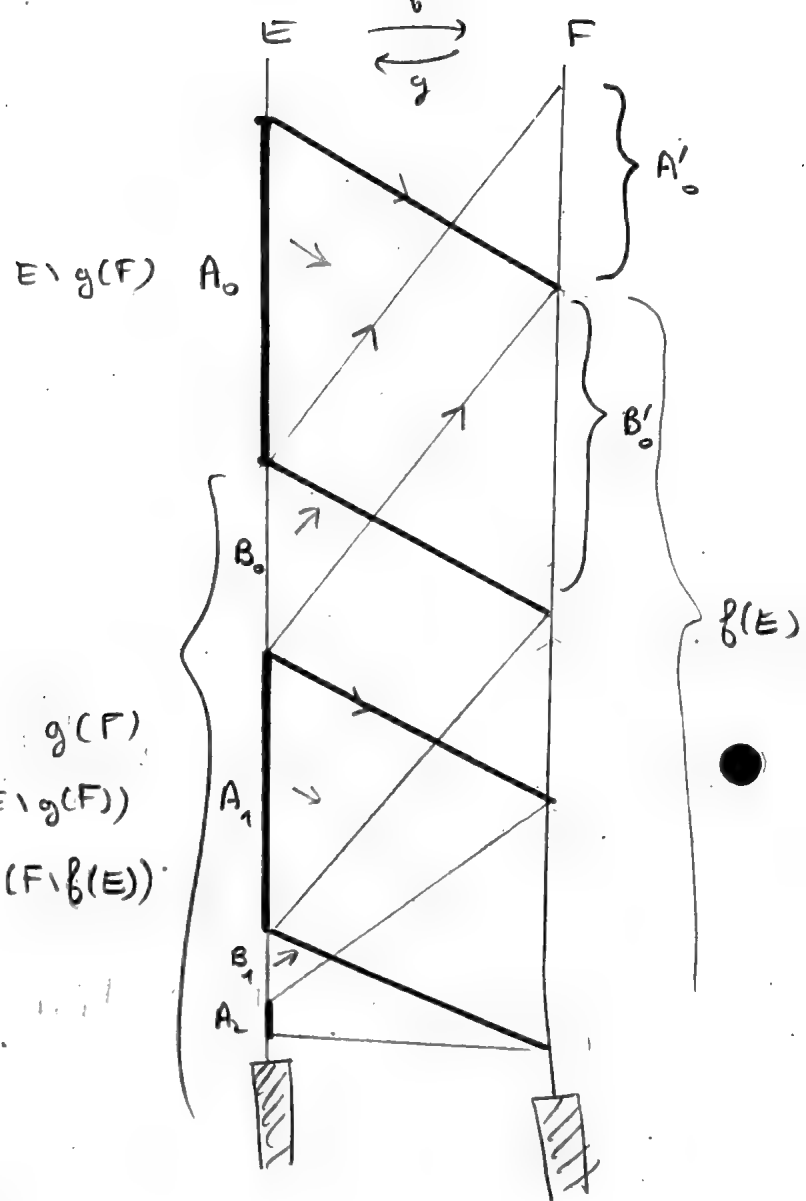
a)

b) \*  $\text{Id}: E \rightarrow E$  est injective, donc  $\text{Card} E \leq \text{Card} E$

\* Théorème de Bernstein: (1890)

$\begin{cases} f: E \rightarrow F \\ g: F \rightarrow E \end{cases}$  injections





$$A_n = (g \circ f)^n (E \setminus g(F))$$

$$B_n = (g \circ f)^n \circ g (F \setminus f(E))$$

$$\text{Soit } C = E \setminus \bigcup_{n \in \mathbb{N}} (A_n \cup B_n)$$

on intervertit  $f$  et  $g$ ,  $E$  et  $F$  :

$$A'_n = (f \circ g)^n (F \setminus f(E))$$

$$B'_n = (f \circ g)^n \circ f (E \setminus g(F))$$

$$C' = F \setminus \bigcup_{n \in \mathbb{N}} (A'_n \cup B'_n)$$

Alors :

$$\left\{ \begin{array}{l} \varphi(A_n) = f \circ (g \circ f)^n (E \setminus g(F)) = (f \circ g)^n \circ f (E \setminus g(F)) = B'_n \\ \text{(c'est vrai grâce à l'associativité de } [f \circ (g \circ f)] \circ \dots \circ (g \circ f) \text{)} \end{array} \right.$$

$$\varphi(B_n) = g^{-1}(B_n) = A'_n$$

1) Les  $A_n, B_n, C$  forment une partition de  $E$  c.à.d.  $A_n \cap B_m = \emptyset$  si  $n \neq m$   
(de même pour  $A'_n, B'_n, C$ )  $\left\{ \begin{array}{l} A_n \cap A_m = \emptyset \\ B_n \cap B_m = \emptyset \end{array} \right.$

2)

$$f(C) = C'$$

\*  $f(C) \subset C'$  si  $f(x) = y$   $x \in C$ , si  $y \notin C'$  on aurait  $y \in B'_n \Rightarrow y = f(A_n) \Rightarrow y = f(x')$   $x' \in A_n$  absurde

• \* ou bien  $y \in A'_n$   $n \geq 1$  (où on  $y \in (F \setminus f(E))$ )

et  $y \in (f \circ g) \circ \dots \circ (f \circ g)(F \setminus f(E)) = f(B'_{n-1})$ .

\*  $f(C) \supset C'$

$$C' \subset f(C) \Rightarrow C' \subset f(E) \Rightarrow F \cap A'_0.$$

$$\text{Soit } y \in C', y = f(x)$$

$$C' \subset f(E) \text{ donc } \exists x \in E / y = f(x) \text{ où } y \in C'$$

$$\begin{cases} \text{Si } x \in A_n, \text{ on aurait } y \in B'_n \\ \text{Si } x \in B_n, \text{ on aurait } y \in A'_{n+1} \end{cases} \text{ donc}$$

Donc  $x \in C$ .

• Ainsi  $f(C) = C'$ , et  $f$  injective  $\Rightarrow f$  bijective de  $C$  sur  $C'$ .

Résultat:  $f$  est bijective de  $E$  sur  $F$

( Remarque: l'ordre  $\leq$  ainsi défini dans la classe des ensembles est une relation de bon ordre. Il existe donc un successeur à  $\mathbb{N}$  pour cette relation. )

⑤ "lemme des cinq" : tous des groupes, tous des homomorphismes.

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \\
 A & \xrightarrow{f} & B & \xrightarrow{g} & C & \xrightarrow{h} & D \xrightarrow{k} E \\
 \downarrow p & & \downarrow q & & \downarrow r & & \downarrow s & & \downarrow t \\
 A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \xrightarrow{h'} & D' \xrightarrow{k'} E' \\
 \downarrow & & & & & & & & \\
 0 & & & & & & & & 
 \end{array}$$

C'est un diagramme commutatif,

$$\begin{cases} q \circ f = f' \circ p \\ r \circ g = g' \circ q \\ \text{etc} \end{cases} \quad r \circ g \circ f = g' \circ q \circ f = g' \circ f' \circ p$$

à lignes exactes : ce qui signifie que toutes les lignes sont des suites exactes.

$$\begin{aligned}
 0 &\xrightarrow{u} A \xrightarrow{f} B \text{ exacte} \Leftrightarrow u \text{ injective} \\
 A &\xrightarrow{f} B \xrightarrow{g} 0 \text{ exacte} \Leftrightarrow f \text{ surjective}
 \end{aligned}$$

a) p surjectif, q et s injectives.

$$x \in C \quad r(x) = 0 \stackrel{?}{\Rightarrow} x = 0$$

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 a & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \xrightarrow{h} D \xrightarrow{k} E \\
 & & & f \mapsto x & & & \\
 \downarrow p & & \downarrow q & & \downarrow r & & \downarrow s & & \downarrow t \\
 a' & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \xrightarrow{h'} D' \xrightarrow{k'} E' \\
 \downarrow & & & & & & & & \\
 & & & & & & & & 0
 \end{array}$$

Soit  $\alpha$  tel que  $\alpha \in C$  et  $\alpha(\alpha) = 0$

$$\text{Si } \alpha(\alpha) = 0 \text{ et } h(\alpha) = 0 \Rightarrow h(\alpha) = 0 \Leftrightarrow \alpha \in \ker h \Rightarrow \exists f \in B / g(f) = \alpha$$

$$G \quad g \circ q(b) = \alpha \circ g(b) \Rightarrow q(b) \in \ker g = \text{Im } f' \Rightarrow \exists a' / f'(a') = q(b)$$

$$\exists a \in A / a' = p(a)$$

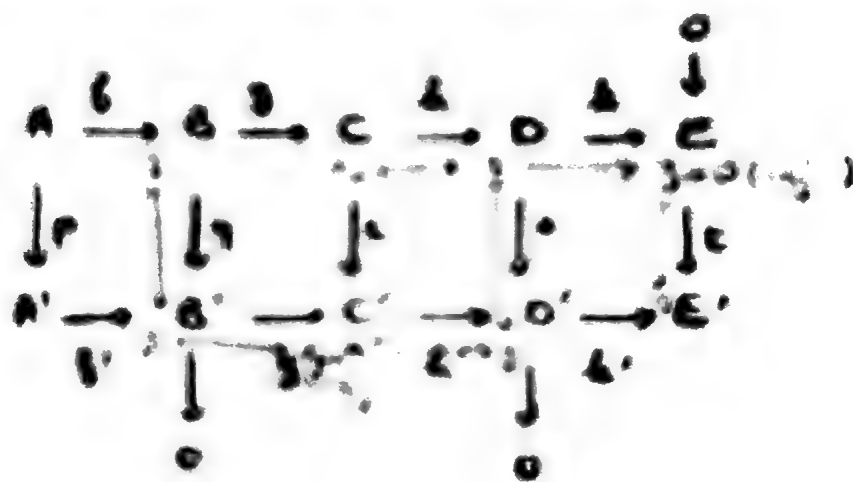
$$q(b) = f' \circ p(a)$$

$$\alpha \circ f' \circ p(a) = q \circ f(a) \Rightarrow f(a) = b \Rightarrow g(b) = 0$$

$$\text{Mais } g(b) = 0 \Rightarrow a' = 0 \Rightarrow a = 0.$$

CQFD

b)  $q$  est surjective,  $f$  injectif  $\Rightarrow$  compatible



$\alpha \in C$  donc  $\exists a \in C / \alpha(a) = \alpha$

$q(a) = \alpha$

$q(a) = \alpha$

$q(a) = \alpha$

$q(a) = \alpha$

$q(a) = \alpha$

Soit  $y' = h'(x')$  surjective:  $\exists y \in D / s(y) = y'$

Alors  $k \circ s(y) = 0 = t \circ k(y)$   
 $\Downarrow$  (injective)  
 $k(y) = 0$

donc  $y \in \ker k = \text{Im } h$

$\exists x_1 \in C / h(x_1) = y$

Notons  $r(x_1) = x'_1$

Mais  $h'(x'_1) = h'(x'_2)$  puisque  $\begin{cases} h'(x'_2) = y' \\ \text{et} \\ s \circ h(x_1) = h' \circ r(x_1) = y' \end{cases}$   
 $\underbrace{s \circ h(x_1)}_y = \underbrace{h' \circ r(x_1)}_{x'_1} = y'$

~~D'où  $h'(x'_1 x'_2) = 0$~~

Pour  $\xi' = x'_1 x'^{-1}$  alors  $h'(\xi') = 0$

Donc  $\xi' \in \ker h' = \text{Im } g' \Rightarrow \exists z' \in B' / g'(z') = \xi'$

$\exists z \in B / q(z) = z'$  puisque  $q$  est surjective

D'où  $\xi' = g' \circ q(z) = r \circ g(z)$

Ainsi  $x'_1 x'^{-1} = r \circ g(z)$

$\Downarrow$

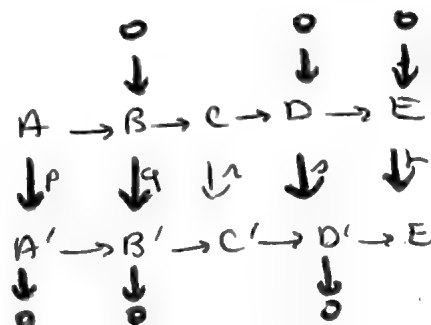
$r(x_1) x'^{-1} = r(g(z))$

$\Downarrow$

$x'_1 = [x_1 g(z)^{-1}]$

$r$  est bien surjective.

c)  $r$  bijectif dès que  $\begin{cases} q, s \text{ bijectives} \\ p \text{ surjectif et } t \text{ injectif} \end{cases}$



③  $H_A = \text{sous-groupe engendré par } A = \bigcap \{H / H \text{ sous-groupe de } G / H \supset A\}$

Alors  $H_A = \{a_1^{\epsilon_1} \dots a_k^{\epsilon_k}, \epsilon_i = \pm 1 \text{ et } a_i \in A \cup \{e\}\}$

( $\square$   $H_A$  est un sous-groupe, et si  $S$  sous-groupe  $S \supset A$  alors  $S \supset H_A$ .  
( $H_A \supset A$ ) donc  $H_A = \text{minimum des } S \text{ contenant } A$ .)

$H_a = \{a^n / n \in \mathbb{Z}\}$  est commutatif.

a) b) facile.

c)  $\Delta(m, n) = 1 \xRightarrow{(1)} G \times H$  cyclique (facile)

$G \times H$  cyclique  $\Rightarrow \Delta(m, n) = 1$

(TB) Supposons que  $G \times H$  soit engendré par  $(x, y)$ . Alors  $x$  engendre  $G$  et  $y$  engendre  $H$ . ~~D'après l'aller~~ D'après l'aller (1),  $(x, y)$  engendre un groupe à  $c = \mu(\underbrace{\omega(x)}_m, \underbrace{\omega(y)}_n)$  éléments.

Donc  $\mu(m, n) = mn \Leftrightarrow \Delta(m, n) = 1$

Remarque:

Tout revient à montrer que le lemme suivant:

$$\omega((x, y)) = \text{ppcm}(\omega(x), \omega(y))$$

Application

$$G = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

#  
Dans  $G$   $\omega((1, 1)) = \text{ppcm}(\omega(1), \omega(1)) = \text{ppcm}(6, 14) = 42$   
donc  $\langle (1, 1) \rangle \neq G$ .

d) classique.

Remarque :

$$G \times H \text{ cyclique} \Leftrightarrow G \text{ cyclique, } H \text{ cyclique} \\ \text{et } \Delta(\#G, \#H) = 1$$

$\Downarrow$

Théorème Chinois

$$\mathbb{Z}/ab\mathbb{Z} \simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ \text{dès que } \Delta(a, b) = 1$$

→ Se rappeler de la résolution du système de congruence :

$$\begin{cases} k \equiv i \pmod{n} \\ k \equiv j \pmod{m} \end{cases}$$

qui admet des solutions si  $\Delta(m, n) = 1$ .

La solution est alors unique modulo  $\text{p.m.c.}(m, n)$

③ a)

$$b) \quad \sigma^2 = 1$$

$$r^n = 1$$

$$r\sigma r = \sigma \Rightarrow r\sigma = \sigma r^{-1}$$

$$H_{\sigma r} = \left\{ \sigma^{n_1} r^{m_1} \dots \sigma^{n_p} r^{m_p} \mid n_i, m_i \in \mathbb{Z} \right\}$$

$$G \text{ peut prendre } \begin{cases} n_i = 0 \text{ ou } 1 \\ m_i = 0, \dots, n-1 \end{cases}$$

Alors  $\Delta_n = \{ \text{Id}, r, r^2, \dots, r^{n-1}, \sigma, \sigma r, \dots, \sigma r^{n-1} \}$  est le groupe engendré par  $r$  et  $\sigma$ .

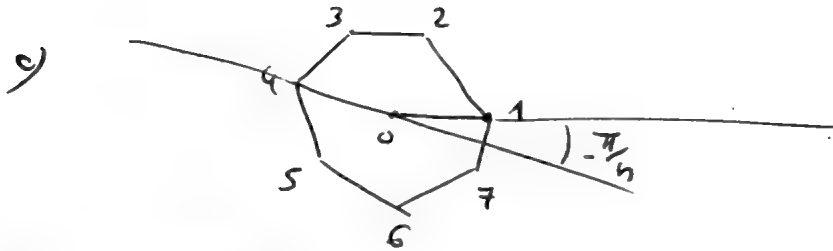
En effet : 1)  $\Delta_n$  est un groupe et  $\Delta_n = \langle r \rangle \cup \sigma \langle r \rangle$

2)  $\Delta_n$  contient  $r$  et  $\sigma$

3)  $\forall G \text{ groupe} \mid G \text{ contient } r \text{ et } \sigma, \Rightarrow G \supset \Delta_n$



Le groupe  $\Delta_n$  possède  $2n$  éléments :



$$H_n = \left\{ e^{\frac{k2i\pi}{n}}, k \in [1, n] \right\} \xrightarrow{\sim} \Delta_n = \{1, \dots, \alpha^{n-1}, \sigma, \dots, \sigma \alpha^{n-1}\}$$

où  $\begin{cases} \alpha = \text{rotation d'angle } \frac{2\pi}{n} \\ \sigma = \text{symétrie par rapport à } D\left(\frac{\pi}{n}\right) \end{cases}$

$\sigma$  est une symétrie orthogonale fixée.

Soit  $\sigma'$  une autre symétrie conservant le polygone régulier

$\sigma^2 \sigma' = \text{rotation d'angle } \alpha \text{ conservant le polygone.}$

d'où  $\sigma' = \sigma \alpha$

(a)  $D(G) = ([G, G]) = \text{groupe engendré par } x^{-1}y^{-1}xy = [x, y] \neq$   
commutateur de  $x, y \in G$ . Remarquons que  $[x, y]^{-1} = [y, x]$

a)  $D(G) \triangleleft G$

$\forall y \in D(G)$

$\forall x \in G \quad x^{-1}yx = y (y^{-1}x^{-1}yx) \in D(G)$

Si  $H \triangleleft G$ , alors  $G/H$  commutatif  $\Leftrightarrow D(G) \subset H$

\* ① On dit que  $G$  est résoluble si il existe des sous groupes  $H_i$  tels que  $\{e\} = H_0 \subset \dots \subset H_n = G$ ,  $H_i \triangleleft H_{i+1}$  (cf ④ feuille 1) et  $H_{i+1}/H_i$  abélien.

a) Montrer que  $G$  résoluble,  $H$  sous groupe de  $G \Rightarrow H$  résoluble.  
et si  $H \triangleleft G$ ,  $G/H$  est résoluble (2<sup>1</sup> pages)

b) Soient  $(i, j, k, r, s)$  5 entiers distincts,  $\sigma = (i, j, k)$ ,  $\tau = (k, r, s)$  des permutations circulaires montrer que  $(k, j, s) = \sigma^{-1} \tau^{-1} \sigma \tau$ .

c) En deduire que si  $N \triangleleft H$  sous groupes de  $S_n$ ,  $H/N$  étant abélien, et si  $H$  contient tous les 3-cycles, ceux ci sont dans  $N$ .

En deduire que si  $n \geq 5$   $S_n$  n'est pas résoluble.

\* ② Calculer l'ordre de  $\sigma = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20)$   
(ie  $n = \inf \{p / \sigma^p = 1\}$ )

\* ③ Soit  $f: A \rightarrow A'$  un homomorphisme de groupe abélien  
 $B \subset A$  un sous groupe d'indice fini. noter  $B \triangleleft A$  ( $A: B$ )  
Montrer que  $(B \triangleleft A) (A: B) = (f(A): f(B)) (\ker f: \ker f|_B)$

\* ④ Soient  $G$  un groupe abélien et  $H, H'$  des sous groupes  
montrer que  $\frac{H+H'}{H'}$  et  $\frac{H}{H \cap H'}$  sont isomorphes

• Soit  $0 \rightarrow G' \rightarrow G^* \rightarrow G'' \rightarrow 0$  une suite exacte  
de groupes (abéliens) montrer que  
 $G^*$  fini  $\Leftrightarrow G'$  et  $G''$  finis et que alors:

$$\# G^* = \# G' \cdot \# G''$$

(\*)  
\* ⑤ On dit que la suite exacte  $0 \rightarrow G' \xrightarrow{f} G \xrightarrow{g} G'' \rightarrow 0$  est scindée si il existe  $s: G'' \rightarrow G$  telle que  $g \circ s = \text{Id}_{G''}$   
Montrer que les conditions équivalentes sont:  
• il existe  $t: G \rightarrow G'$  telle que  $t \circ f = \text{Id}_{G'}$   
• il existe un sous groupe  $H$  de  $G$  tel que  $G = G' \oplus H$   
(et alors  $G'' \cong H$ )

à évaluer  
ainsi que  
feuille TD  
n° 1 et 2

à  
comparer.

$$(x) \bullet \quad H \triangleleft K_1 \triangleleft K_2 \quad \left(K'_1 = K_1/H\right) \triangleleft \left(K'_2 = K_2/H\right) \text{ et } K'_2/K'_1 \simeq K_2/K_1$$

Si  $H \triangleleft G$

a)  $G$  résoluble  $\Leftrightarrow H$  et  $G/H$  sont résolubles.

$$(\Rightarrow) \textcircled{a} \quad 0 \subset H_1 \cap H \subset \dots \subset H_n \cap H = H$$

$$H_i \cap H \triangleleft H_{i+1} \cap H$$

$$y \in H_i \cap H \\ x \in H_{i+1} \cap H \Rightarrow x^{-1}yx \in H_i \cap H$$

$$\text{et } \frac{H_{i+1} \cap H}{H_i \cap H} \text{ abélien } \begin{cases} x \in H_{i+1} \cap H \\ y \in H_{i+1} \cap H \end{cases}$$

$$x^{-1}y^{-1}xy \in H_i \cap H \Rightarrow \frac{H_{i+1} \cap H}{H_i \cap H} \text{ commutatif.} \\ (\text{c.a.d. } [\bar{x}, \bar{y}] = \bar{e})$$

préliminaire

$$\text{On a : } D(G/H) \simeq \frac{D(G)}{D(G) \cap H}$$

$$D(G) \xrightarrow{\alpha'} D(G/H) \subset G/H \\ [x, y] \longmapsto [\bar{x}, \bar{y}] = \overline{[x, y]}$$

$\alpha'$  est la restriction  
de  $\alpha : G \rightarrow G/H$

$\alpha'$  surjective

$$\begin{array}{ccc} & & \nearrow \alpha' \\ & \downarrow & \\ D(G) & & \end{array}$$

$\text{Ker } \alpha'$

or  $\text{Ker } \alpha' = D(G) \cap H (= \text{Ker } \alpha \cap D(G))$  et  $D(G) \cap H$  distingué

$$D(G/H) \simeq \frac{D(G)}{D(G) \cap H}$$

$$D(G/H) \simeq \frac{D^2(G)}{D^2(G) \cap (D(G) \cap H)} \simeq \frac{D^2(G)}{D^2(G) \cap H}$$

Par récurrence :

$$D^i(G/H) \simeq \frac{D^i(G)}{D^i(G) \cap H}$$

montrons que  $G/H$  résoluble dès que  $G$  résoluble

$$\exists n \mid D^n(G/H) \cong \frac{D^n(G)}{D^n(G) \cap H} = \frac{\{e\}}{\{e\} \cap H} = \{e\}$$

$$(\Leftarrow) \text{ Réciproquement, } G/H \text{ résoluble} \Rightarrow D^n(G)/D^n(G) \cap H = \{e\}$$

$$\text{d'où } D^n(G) \subset H \text{ et } H \text{ résoluble} \Rightarrow \exists n' \mid D^{n'}(H) = \{e\}$$

$$\text{d'où } D^{n'+n}(G) \subset D^{n'}(H) = \{e\} \Rightarrow D^{n'+n}(G) = \{e\}$$

ce qui montre que  ~~$D^{n'+n}(G)$~~   $G$  est résoluble.

Autre démonstration :

$$\{e\} = H_0 \subset H_1 \subset \dots \subset H_n \stackrel{H}{=} H$$

$$G' = G/H$$

$$\{e\} = H'_0 \subset H'_{n+1} \subset \dots \subset H'_{n+k} = G'$$

Il y a une bijection croissante de l'ensemble des sous-groupes de  $G/H$  dans l'ensemble des sous-groupes de  $G$  qui contiennent  $H$ .

$$H'_i \subset G' = G/H$$

Il existe  $H_i$  sous-groupe de  $G$  tel que  $H \subset H_i \subset G$

$$\text{et } H'_i = H_i/H \quad (H \triangleleft H_i \text{ car } H \triangleleft G)$$

Plus :

$$e = H_0 \subset \dots \subset H_n = H \subset H_{n+1} \subset \dots \subset H_{n+k} = G$$

Remarque :

$$G' = G/H \quad \text{où } H \triangleleft G$$

Il existe une bijection

$$\{K' / K' \subset G', \text{ sous-groupe de } G'\} \longrightarrow \{K \subset G \text{ tel que } K \supset H\}$$

sous-groupe

de plus,  $K$  distingué ssi  $K'$  distingué.

preuve:

On prend  $K' \longrightarrow \varphi^{-1}(K') = \{x \in G / x = \varphi(n) \in K'\} = K$

$$K/H \xleftarrow{\varphi} K$$

$$\begin{cases} \varphi(\varphi^{-1}(K')) = K' \text{ donc } \varphi \text{ surjective.} \\ \varphi^{-1}(\varphi(K)) \supseteq K. \text{ On a l'égalité, car :} \end{cases}$$

$$\begin{aligned} x \in \varphi^{-1}(\varphi(K)) &\Leftrightarrow \varphi(x) \in \varphi(K) \Leftrightarrow \exists y / \varphi(x) = \varphi(y) \quad y \in K \\ &\Leftrightarrow \varphi(xy^{-1}) = e \quad y \in K \Leftrightarrow \underline{xy^{-1} \in H \subset K} \end{aligned}$$

$$\Leftrightarrow \text{d'où } x \in K.$$

$$\text{Donc } \varphi^{-1}(\varphi(K)) = K$$

$$K/H = K'$$

The  $1^\circ \underline{K \triangleleft G \quad H \subset K \subset G \Rightarrow K' \triangleleft G'}$

$$\begin{matrix} x \in G' \\ y \in K' \end{matrix} \quad x^{-1}y x = \overbrace{x^{-1}y x}^{\varphi(n)} \quad \text{où } y \in K \text{ et } x \in G$$

comme  $x^{-1}y x \in K \Rightarrow x^{-1}y x \in K'$  donc  $K'$  distingué.

$$2^\circ \quad \underline{K' \triangleleft G' \Rightarrow K \triangleleft G}$$

$$\begin{array}{l} y \in K \\ x \in G \end{array} \quad x^{-1}yx \quad \overline{x^{-1}yx} = \bar{x}^{-1}\bar{y}\bar{x} \in K' \text{ car } K' \text{ distingué.}$$

$$\text{donc } x^{-1}yx \in K \Rightarrow K \triangleleft G$$

$$(2) \quad \sigma = (1, 3, 11, 12, 8) \circ (2, 15, 10) \circ (4, 6, 13, 9) \circ (5) \circ (7, 14)$$

$$\sigma^n = \prod_{i=1}^k \sigma_i^n$$

$$\sigma^n|_{E_i} = \sigma_i \quad \text{donc} \quad \sigma^n = \text{Id} \Leftrightarrow \sigma_i^n = \text{Id} \quad i=1, \dots, k$$

$$\Updownarrow$$

$$\forall i \quad n_i | n \quad \text{où } n_i = \text{ordre de } \sigma_i$$

$$\Updownarrow$$

$$\text{ppcm}(n_1, \dots, n_k) | n$$

l'ordre de  $\sigma$  est le  $\text{ppcm}(n_1, \dots, n_k)$ .

$$\text{ici : } \text{ppcm}(5, 3, 4, 2) = 60$$

Remarque :  $\sigma = \sigma_1 \circ \sigma_2 \circ \dots \circ \sigma_k$  dans  $\mathcal{S}_8$

$$n_1 \geq \dots \geq n_k$$

$n_1 = 8$	ordre de $\sigma = 8$
7	7
6	6
5	(15)
4	12
3	3

④ 1°/  $(H+H')/H \simeq H/H \cap H'$

La suite  $0 \rightarrow H \cap H' \xrightarrow{\alpha} H \xrightarrow{\beta} H+H'/H \rightarrow 0$  est exacte.

$$x \mapsto \alpha(x) = x$$

$$x \mapsto \pi_{H'}$$

Remarque: Montrer que si  $H \triangleleft G$  (non forcément commutatif), on a :

1)  $HH'$  est un sous-groupe de  $G$ .

$$2) \boxed{HH'/H \simeq H/H \cap H'}$$

$$2^\circ \quad 0 \rightarrow G' \xrightarrow{\alpha} G \xrightarrow{\beta} G'' \rightarrow 0$$

$$\begin{array}{ccc} & & \uparrow \bar{\beta} \\ & \cup & \\ \alpha \searrow & & \nearrow \\ & \alpha(G') & \\ & \searrow & \\ & G/\alpha(G') & \end{array}$$

1)  $G$  fini  $\Leftrightarrow G'$  et  $G''$  finis

$\alpha(G') = \ker \beta$  sous-groupe distingué de  $G$ .

$\bar{\beta}$  est un isomorphisme de groupes.

Donc  $G'' \simeq G/\alpha(G') \quad (1)$

(1):  $G$  fini  $\Rightarrow \alpha(G')$  fini et  $G''$  fini

$$\uparrow \uparrow (\text{car } \alpha: G' \xrightarrow{\sim} \alpha(G'))$$

$G'$  fini et  $G''$  fini.

Inversement, si  $G'$  et  $G''$  sont finis, alors  $G/\alpha(G')$  fini et  $\alpha(G')$  fini.

Ainsi  $G = \bigsqcup_{\alpha \in G/\alpha(G')} \pi^{-1}(\alpha)$  où  $\pi$  est la surj. can. de  $G$  sur  $G/\alpha(G')$ .  
 $\alpha \in G/\alpha(G')$  fini, de cardinal  $|\alpha(G')|$

donc  $G$  est fini.

2)  $\#G = \#G' \cdot \#G''$

Si  $G$  est fini,  $G'' \simeq G/\alpha(G') \Rightarrow \#G'' = \frac{\#G}{\#\alpha(G')} = \frac{\#G}{\#G'}$

(CQFD)



③ On utilise le ④.

$$0 \rightarrow \ker f / \ker f|_B \xrightarrow{\varphi} A/B \xrightarrow{\psi} f(A)/f(B) \rightarrow 0 \quad (1)$$

$$\begin{aligned} \tilde{x} &\longmapsto \dot{x} + \dot{b} = \dot{x+b} \\ x &\longmapsto \overline{f(x)} \end{aligned}$$

• Les  $\varphi$  sont bien définies :  $\tilde{x} = \tilde{y} \Leftrightarrow x - y \in \ker f|_B = B \cap \ker f$   
 $\Rightarrow \tilde{x} = \tilde{y}$

et  $\tilde{x} = \tilde{y} \Leftrightarrow x - y \in B \Rightarrow f(x) - f(y) \in f(B)$   
 c'est-à-dire  $\overline{f(x)} = \overline{f(y)}$

• (1) est une suite exacte :

$$\begin{aligned} * \quad & \left\{ \begin{aligned} \ker \varphi &= \{ \tilde{x} \in A/B \mid f(x) \in f(B) \} \\ \operatorname{Im} \varphi &= \{ \tilde{x} \in A/B \mid \exists b \in B \quad x+b \in \ker f \} = \{ \tilde{x} \in A/B \mid f(x) \in f(B) \} \end{aligned} \right. \end{aligned}$$

\*  $\varphi$  injective :  $\tilde{x} = 0 \Leftrightarrow x \in B$

ou  $x \in \ker f \Rightarrow x \in B \cap \ker f = \ker f|_B \Rightarrow \tilde{x} = 0$

\*  $\varphi$  surjective : évident.

② après le ③ :  $\ker f / \ker f|_B$  et  $f(A)/f(B)$  sont finis et :

$$[A : B] = [f(A) : f(B)] \times [\ker f : \ker f|_B]$$



1)  $\Rightarrow$  2)

$$0 \rightarrow G' \xrightarrow{\beta} G \xrightarrow{g} G'' \rightarrow 0$$

$\downarrow$   
 $\iota$

$\beta(G') \simeq G'$  car  $\beta$  est injective.

Soit  $H = \ker \iota$

Alors  $G = \beta(G') \oplus \ker \iota$

[En effet:  $\bullet x \in \beta(G') \cap \ker \iota \quad \left\{ \begin{array}{l} \iota(x) = 0 \\ x = \beta(x') \end{array} \right. \Rightarrow \iota \circ \beta(x') = x' = 0 \Rightarrow x = 0$

$\bullet \forall x \in G \quad x = \underbrace{\beta(\iota(x))}_{\in \beta(G')} + \underbrace{(x - \beta(\iota(x)))}_{\in \ker \iota} \Rightarrow G = \beta(G') + \ker \iota$ ]

2)  $\Rightarrow$  Def On suppose que  $G = \beta(G') \oplus H$ . Comme  $\beta(G') = \ker g$ ,

$G = \ker g \oplus H$

$$G \xrightarrow{g} G'' \rightarrow 0$$

$\downarrow$   
 $\iota$

$\forall x'' \in G'' \quad \exists! x \in H \quad g(x) = x'' \quad (\text{cf. } g(x) = g(y) \Leftrightarrow x - y \in H \cap \ker g = \{0\})$

Posons  $\Delta(x'') = x$

Alors:  $\Delta$  est un homomorphisme et  $g \circ \Delta(x'') = g(x) = x''$  c.q.f.d.

exercice supplémentaire: Sur  $G' \times G'' = G$

$(x', x'')(y', y'') = (x' \alpha_{x''}(y'), x'' y'')$  (produit semi-direct)

\* c'est une loi de groupe

\* On a une suite exacte scindée

$0 \rightarrow G' \rightarrow G \rightarrow G'' \rightarrow 0$

(où  $G'' \rightarrow \text{Aut } G'$   
 $x'' \mapsto \alpha_{x''}$   
est un homomorphisme)

Remarque 1:  $0 \rightarrow A_n \rightarrow \mathcal{I}_n \xrightarrow{\epsilon} \{-1, +1\} \rightarrow 0$   
est scindée (ou scindée)

$\Delta(+1) = \text{Id}$

$\Delta(-1) = \tau$  transposition.

Remarque 2 :

$$0 \rightarrow \mathcal{O}^+(Z) \rightarrow \mathcal{O}(Z) \rightarrow \{\pm 1\} \rightarrow \{1\}$$

$$\sigma(x, y) = (-x, y)$$

\* ① a) Montrer que si  $p \in \mathbb{N}$  est premier  $\mathbb{Z}/p\mathbb{Z}$  est un corps (noté  $K$ )

b) Ainsi  $(\mathbb{Z}/p\mathbb{Z} - \{0\})$  est un groupe pour la multiplication

on se propose de montrer que ce groupe est cyclique:

(i) Soit  $(p-1) = q_1^{\beta_1} \dots q_s^{\beta_s}$  une décomposition en facteurs irréductible, montrer que  $\forall x \in K - \{0\} \quad x^{p-1} = 1$

(ii)  $\frac{p-1}{q_i} \in \mathbb{N}$  est inférieur strictement à  $p-1$ ; en déduire l'existence de  $x_i \in K - \{0\}$  non racine de  $x^{\frac{p-1}{q_i}} - 1$

(i.e.  $x_i^{\frac{p-1}{q_i}} \neq 1$ )

(iii) En conclure que  $y_i = x_i^{\frac{p-1}{q_i \beta_i}}$  est d'ordre  $q_i^{\beta_i}$  dans  $(K - \{0\})$  puis que  $y_1 \dots y_s = y$  engendre  $K$ .

(NB. Ultérieurement on montrera peut-être que tout corps fini est commutatif d'ordre  $p^n$ ,  $p$  premier et que  $K - \{0\}$  est cyclique.)

\* ② Soit  $G$  un groupe commutatif fini, noté multiplicativement  $n \in \mathbb{N}$  tel que  $\forall x \in G \quad x^n = e$

a) Soit  $n = rs$ ,  $r, s$  premiers entre eux.

-  $M = \{x \in G \mid x^r = e\}$ ,  $N = \{x \in G \mid x^s = e\}$  sont des sous-groupes de  $G$ .

- Montrer que  $N \times N \rightarrow G$  est un isomorphisme.  
 $(x, y) \rightarrow xy$

b) Soit  $n = p_1^{\alpha_1} \dots p_k^{\alpha_k} = q_1 \dots q_k$ ,  $p_i$  premiers, la décomposition en facteurs irréductibles de  $n$ .  $q_i = p_i^{\alpha_i}$ . Alors  $G$  est isomorphe au produit direct des  $H_i = \{x, x^{q_i} = e\}$   
 $\cong \prod G(p_i)$

c) Soit  $G$  un groupe comm. fini  $n \in \mathbb{N}$ ,  $p$  premier tel que:  $\forall x \in G \ x^{p^2} = e$ .

Montrer que  $\# G$  est une puissance de  $p$ .

d) En déduire que si  $\# G = n = p_1^{r_1} \dots p_k^{r_k}$ ,  $p_i$  premiers distinct,  $G$  est isomorphe au produit direct de  $k$  groupes d'ordre  $p_i^{r_i}$ .

(3)  $(G, +)$  groupe commutatif muni d'une relation d'ordre  $\leq$  et dit ordonné si:  $\forall x, y, z \in G$

$$x \leq y \Rightarrow x + z \leq y + z$$

1) Montrer que  $G$  est ordonné  $\Leftrightarrow P + P \subseteq P$  et  $P \cap (-P) = \{0\}$   
 un groupe ordonné  
 tel que  $P = \{x / x \geq 0\}$

2) Décrire  $P$  lorsque  $\leq$  est l'ordre lexicographique (resp. l'ordre produit sur  $\mathbb{Z}^2$ ). (vérifier que ces ordres munissent  $G$  d'une structure de groupe ordonné)

3) L'ordre est total ssi  $P \cup (-P) = G$ .

4) Déterminer toutes les structures de groupe ordonné sur un groupe cyclique (fini, c'est trivial, ou infini c'est plus intéressant...)

(4) Soit  $A$  un sous groupe de  $G$ .  
 on note  $N(A) = \{g \in G \mid g^{-1} A g = A\}$  normalisateur de  $A$

$$Z(A) = \{a \in A, \forall a' \in A \ a a' = a' a\}$$

montrer que  $N(A)$  et  $Z(A)$  sont des sous groupes de  $G$  et que  $Z(A) \triangleleft N(A)$  ( $A \triangleleft N(A)$  aussi!).

(5) Interpréter  $N(A)$  en termes de l'action de  $G$  sur lui-même

$$G \times G \rightarrow G$$

$$g, g' \mapsto \sigma(g)(g') = g g' g^{-1}$$

(Montrer que  $N_x = \{g \in G \mid x g x^{-1} = x\}$  est un sous groupe)

① a) facile (connue!)  $F_p = \mathbb{Z}/p\mathbb{Z}$  est un corps.

b) i) facile

ii)

$$p-1 = q_1^{\beta_1} \dots q_s^{\beta_s} \quad \beta_i > 0; q_i \in \mathcal{P}$$

$$\exists x_i \in G = \mathbb{Z}/p\mathbb{Z} \setminus \{0\} \quad / \quad x_i^{\frac{p-1}{q_i}} \neq 1$$

Le polynôme  $X^{\frac{p-1}{q_i}} - 1$  a au plus  $\frac{p-1}{q_i} < p-1$  racines. Comme  $\#G = p-1$ , l'existence de  $x_i$  est prouvée.

$$iii) y_i = x_i^{\frac{p-1}{q_i^{\beta_i}}}$$

$$y_i^{q_i^{\beta_i}} = 1 \Rightarrow \omega(y_i) \mid q_i^{\beta_i} \Rightarrow \omega(y_i) = q_i^{\alpha_i} \quad \alpha_i \leq \beta_i$$

$$\text{Si } \alpha_i < \beta_i, \text{ on aurait } y_i^{q_i^{\beta_i-1}} = 1.$$

$$\text{Ici, nous avons } y_i^{q_i^{\beta_i-1}} = x_i^{\frac{p-1}{q_i^{\beta_i}} q_i^{\beta_i-1}} = x_i^{\frac{p-1}{q_i}} \neq 1, \text{ donc } \alpha_i = \beta_i.$$

$$\text{Ainsi : } \boxed{\omega(y_i) = q_i^{\beta_i}} \text{ dans } G \setminus \{0\}$$

$$\text{On prend } y = y_1 \dots y_s$$

$$y^{\frac{p-1}{q_i}} \neq 1 \text{ pour tout } i, \text{ de sorte que } \omega(y) = p-1.$$

$$\text{Montrons que } y^{\frac{p-1}{q_i}} \neq 1$$

$$y^{\frac{p-1}{q_i}} = \underbrace{y_1^{\frac{p-1}{q_i}}}_{=1} \dots y_i^{\frac{p-1}{q_i}} \dots \underbrace{y_s^{\frac{p-1}{q_i}}}_{=1}$$

$$\text{car } \omega(y_s) = q_s^{\beta_s} \mid \frac{p-1}{q_i}$$

$$y^{\frac{p-1}{q_i}} = y_i^{\frac{p-1}{q_i}} \neq 1 \text{ car } q_i \nmid \frac{p-1}{q_i} \text{ (où } q_i^{\beta_i} = \omega(y_i))$$

Conclusion:  $y$  engendre  $(F_p \setminus \{0\}, \times)$

Remarque : 1)  $x, y \in G$   $G$  est un groupe d'ordre  $n$ .

$$\omega(xy) = \omega(x)\omega(y) \text{ si } \Delta(\omega(x), \omega(y)) = 1.$$

2)  $K$  corps fini.  $\{n.1 / n \in \mathbb{Z}\} \simeq \mathbb{F}_p$  où  $p$  = caractéristique du corps  $K$ .  $\mathbb{F}_p \subset K$   $K$  est donc un surcorps de  $\mathbb{F}_p$ , il peut être considéré comme un es sur  $\mathbb{F}_p$ :  $K \simeq (\mathbb{F}_p)^\wedge$

$$\text{Ainsi } \#K = p^n \text{ et } \dim_{\mathbb{F}_p} K = n$$

• Il existe, à isomorphisme près, un unique corps  $\mathbb{F}_{p^n}$ ;  $\# \mathbb{F}_{p^n} = p^n$ ;  
et  $K \setminus \{0\}$  est un groupe cyclique.



Exercice Déterminer les groupes à 8 éléments. ( $8=2^3$ ) (à isomorphisme près) 5

Solution:  $n = \# G = 8$

$p = \# Z(G) = 2$  ou  $4$  ou  $8$  (car  $\# Z(G) \equiv 0 \pmod{p}$  si  $G = p$ -groupe)

•  $p = 8$ :  $G$  est commutatif, donc de la forme  $\mathbb{Z}/8\mathbb{Z}$  ou  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

ou  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

•  $p = 4$ :  $Z(G) = \{e, x_1, x_2, x_3\}$

$G = \{e, x_1, x_2, x_3\} \cup \{g, gx_1, gx_2, gx_3\}$  où  $g \notin Z(G)$

Plus  $gx_1gx_2 = g^2x_1x_2 = g^2x_2x_1 = gx_2gx_1$

et la loi est commutative dans  $G$  ! Ce qui est absurde.  
Ce cas est impossible.

•  $p = 2$ :

$0 \rightarrow Z(G) \hookrightarrow G \xrightarrow{\leftarrow} G/Z(G) \rightarrow 0$  est exacte.

$\# G/Z(G) = 4$  et il n'y a que 2 types de groupes à 4 éléments (tous commutatifs). De 2 choses l'une:

\* Si  $G/Z(G) \cong \mathbb{Z}/4\mathbb{Z}$ , soit  $a \in G$  /  $\bar{a}$  engendre  $G/Z(G)$ .

$\omega(a) = 4$  ou  $8$ . Ce ne peut être  $8$  car sinon  $G$  commutatif.

Donc  $\omega(a) = 4$ , et on peut scinder la suite ( $\leftarrow$ )

$(a) \xrightarrow{\sim} \mathbb{Z}/4\mathbb{Z}$

Plus  $\forall g \in G \exists ! z \in Z(G) \exists ! i \in [0, 1, 2, 3] / g = za^i$

(puisque suite scindée  $\Rightarrow G = Z(G) * G/Z(G)$ , ou  $Z(G) \trianglelefteq G$ )

(En effet:  $\bar{g} = \bar{z} \bar{a}^i \Rightarrow g = a^i z$  où  $z \in Z(G)$ .)

Donc  $G$  est commutatif  $[(za^i)(z'a^j) = (z'a^j)(za^i) \text{ car } z, z' \in Z(G)]$

Ce qui est absurde. Donc:

\*  $G/Z(G) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

		b
a	ab	

$Z(6)$  {

$Z(6)$

	1	-1	i	-i	j	-j	k	-k
1	1	-1	i	-i	j	-j	k	-k
-1	-1	1	-i	i	-j	j	-k	k
i	i	-i	-1	1	k	-k	-j	j
-i	-i	i	1	-1				
j	j	-j						
-j	-j	j						
k	k	-k						
-k	-k	k						

$i \cdot j = k$

On a :  $G/Z(6) = \{1, i, j, k\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \Rightarrow \begin{cases} ij = k \\ i^2 = j^2 = k^2 = 1 \end{cases}$   
on peut supposer que  $ij = k$  (c'est la structure de  $G/Z(6) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  qui nous le donne  $\exists : ij = \pm k, \dots$ )

$i^2 = 1 \Leftrightarrow i^2 \in Z(6) = \{1, -1\}$ . Si  $i^2 = 1$ , alors

~~$\{1, i, j, k\}$  est un sous-groupe de  $G$  car :~~

$$\begin{aligned} \cancel{i^2} &= 1 \\ \cancel{j^2} &= k \\ \cancel{ij} &= k \end{aligned}$$

On veut montrer que  $\begin{cases} i^2 = j^2 = k^2 = -1 \\ ij = k \\ jk = i \\ ki = j \end{cases}$

Si  $i^2 = j^2 = k^2 = 1$ , alors  $ij = k \Rightarrow ij = ji$  etc et  $G$  commutatif.

On peut donc supposer que  $i^2 = -1$ .

(autre façon de le voir : si tout élément de  $G$  est d'ordre 2, alors  $G$  est commutatif.

En effet :   
 ~~$abba = a b^2 a = a a = a^2 = 1$  d'où  $abba = 1 \Rightarrow abb = a$~~   
 ~~$a^2 = 1 \Rightarrow b^2 = 1$  alors  $(ab)^{-1} = b^{-1} a^{-1} = ba$~~   
 et  $abba = 1 \Rightarrow (ab)^{-1} = ba \Rightarrow ab = ba$  )  
 " car  $(ab)^2 = 1$

$$G/Z(G) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Soit  $i \in G$  d'ordre 4  $i \neq 1$   $i^2 \in Z(G) = \{\pm 1\} \Rightarrow i^2 = -1$

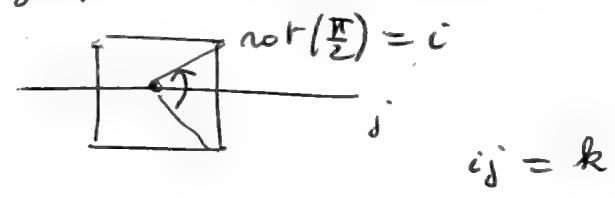
$$G/Z(G) = (1, \bar{i}, \bar{j}, \bar{k}) \quad ij = k$$

1-cas  $j^2 = 1$  \* Si  $k^2 = 1$ , on trouve  $D_4$  on tombe sur une contradiction. En effet : on construit la table :

~~$$\begin{cases} ij = k \Rightarrow jk = i \Rightarrow ki = j \\ ij = k \Rightarrow ik = -j \\ jk = i \Rightarrow ji = -k \end{cases}$$~~

$$\begin{cases} kj = i & jk = -i \\ ik = -j & ki = j \\ ij = k & ji = -k \end{cases}$$

On a la table du groupe : c'est le groupe diédral  $D_4$ , ou "groupe du carré".



\* Si  $k^2 = -1$ , on tombe sur une contradiction.

On a :

$$\begin{cases} i^2 = -1 \\ j^2 = 1 \\ k^2 = -1 \end{cases} \quad ij = k$$

$jk = i$	$kj = i$
$ik = -j$	$ki = -j$
$ij = k$	$ji = k$

donc  $i, j, k$  commutent entre eux. On tombe sur  $G$  commutatif. Absurde puisque  $\#Z(G) = 2$ .

2-cas  $j^2 = -1$  \* si  $k^2 = -1$ , on a  $i^2 = j^2 = k^2 = -1$

on écrit que  $G$  est isomorphe au groupe des quaternions :  $\mathbb{Q} = \mathbb{R}^4$  muni d'une multiplication donnant (\*) :

$$(*) \begin{cases} ij = k & jk = i & ki = j \\ ji = -k & kj = -i & ik = -j \end{cases}$$

$(x + yi + zj + tk)(x' + y'i + z'j + t'k) =$  à développer.  $\mathbb{Q}$  = corps des quaternions.

Exercice: Soit  $G = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in K \text{ corps} \right\}$  Montrer que  $G$  est un groupe pour  $\times$ , et que  $M_{a,b,c} \in Z(G) \Leftrightarrow a=b=0$ .

$\Rightarrow$  Vérifier que  $G/Z(G)$  est commutatif (ind:  $M_{a,b,c} \in M_{a,b,0}(Z(G))$ )

$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a' & c' \\ 0 & 1 & b' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a'+a & c'+ab'+c \\ 0 & 1 & b'+b \\ 0 & 0 & 1 \end{pmatrix}$$

la loi est interne. Cherchons l'inverse de  $M_{a,b,c}$ :

$$\begin{cases} a'+a=0 \\ c'+ab'+c=0 \\ b'+b=0 \end{cases} \Leftrightarrow \begin{cases} a'=-a \\ b'=-b \\ c'=-c+ab \end{cases} \quad \begin{array}{l} \text{existe et est unique.} \\ \text{et } \in G. \end{array}$$

él. neutre:  $\text{Id}$ .

Centre de  $G$ ? On cherche  $(a,b,c)$  tels que  $\forall a', b', c'$  on ait:

$$\begin{cases} a'+a = a+a' \\ c'+ab'+c = c+ab'+c \\ b'+b = b+b' \end{cases} \Leftrightarrow \begin{array}{l} a'b + b'(-a) = 0 \\ \Downarrow \\ b=a=0 \\ \text{cqfd} \end{array} \quad \forall a', b', c'$$

- ① Soit  $G$  un groupe d'ordre  $p^k$ ,  $p$  premier
- montrer que  $Z(G) \neq \{e\}$ . ( $Z(G)$  centre de  $G$ )
  - Montrer que tout groupe d'ordre  $p^2$  est commutatif
- ② Un groupe est simple si  $H \triangleleft G$  implique  $H = \{e\}$  ou  $G$
- Montrer qu'un groupe d'ordre 220 admet un seul 11-groupe de Sylow. En déduire que  $G$  n'est pas simple.
- Montrer qu'un groupe d'ordre 15, 20, 30, 48, 36, 96, 160, 56 ou  $p^2 m$  ( $p^2 > m$ ,  $p$  premier) n'est pas simple.
- ③ Dédurre de ①a) que tout groupe d'ordre  $p^k$  est <sup>non</sup> simple dès que  $k > 1$  ~~( $k > 1$ )~~

- ④ a) Soit  $G$  un groupe opérant transitivement sur un ensemble  $E$
- Montrer l'équivalence des deux propriétés i) et ii) suivantes
- Tout stabilisateur  $H_x$  est un sous groupe maximal.
  - Si  $F \subset E$  satisfait  $\forall g \in G (g.F \subset F \text{ ou } g(F) \cap F = \emptyset)$  alors  $F = E$  ou  $\#F = 1$ .
- un tel  $G$  est dit primitive
- b)  $G$  est dit n-transitif sur  $E$  si :
- (P<sub>n</sub>)  $\left\{ \begin{array}{l} \text{quelque soient } (a_1, \dots, a_n), (b_1, \dots, b_n) \text{ dans } E, \text{ avec} \\ a_i \neq a_j, b_i \neq b_j \text{ si } i \neq j; \text{ il existe } \sigma \in G \text{ tel que} \\ \sigma(a_i) = b_i. \end{array} \right.$
- ~~et si (P<sub>n+1</sub>) est~~
- Montrer que :
- $P_2 \Rightarrow P_{2-1}$
  - $G_n$  est  $n$ -transitif,  $A_n$   $n-2$  transitif
  - $n > 1 \Rightarrow G$  est primitif

$$G \trianglelefteq \tilde{G} E.$$

c) Soit  $G$  primitif,  $N \triangleleft G$  sous groupe normal propre alors  $N$  est transitif. (considérer  $F = N \cdot x$  pour tous  $x \in E$ )

d) On veut montrer que  $A_5$  est simple.

Soit  $1 \neq N \triangleleft A_5$ . Montrer que  $N$  contient un sous groupe cyclique engendré par  $(1, 2, 3, 4, 5) = \sigma$

-  $\tau = (1, 2, 3)$  montrer que  $\tau \sigma \tau^{-1} \neq \sigma$

En déduire que  $N$  contient 6 sous groupe de Sylow.

- Montrer que si  $\# N = 30$ ,  $N$  contient 24 éléments d'ordre 5, en déduire une contradiction.

(5)

On désigne par  $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$  l'ensemble obtenu en complétant  $\mathbb{C}$  par un «point à l'infini». On appelle *homographie* l'application  $f$  de  $\hat{\mathbb{C}}$  dans lui-même définie par les nombres complexes  $a, b, c, d$ ,  $ad - bc \neq 0$  telle que:

$$c \neq 0 \quad \begin{cases} f(z) = \frac{az+b}{cz+d} & \text{si } z \neq \infty \text{ et } z \neq -\frac{d}{c} \\ f(\infty) = \frac{a}{c}, \quad f\left(-\frac{d}{c}\right) = \infty \end{cases}$$

$$c = 0 \quad \begin{cases} f(z) = \frac{a}{d}z + \frac{b}{d} & \text{si } z \neq \infty \\ f(\infty) = \infty. \end{cases}$$

Si les points invariants sont distincts, l'homographie sera dite *non parabolique* (parabolique dans le cas contraire).

**Question 1.** — Montrer que l'ensemble  $G$  des homographies est un groupe (dit *circulaire*), opérant sur  $\hat{\mathbb{C}}$  et que l'ensemble  $H$  des homographies vérifiant  $ad - bc = 1$  est un sous-groupe de  $G$ .

**Question 2.** — a) Montrer qu'une homographie [parabolique, distincte de l'identité, engendre dans  $H$  un sous-groupe cyclique infini.

b) Soit  $\Gamma$  un sous-groupe fini de  $H$ . Montrer que si tous les éléments de  $\Gamma$  ont même point invariant  $\alpha$  alors  $\Gamma$  est un groupe cyclique. En déduire que tous les éléments de  $\Gamma$  ont mêmes points invariants.

**Question 3.** — Soit  $\Gamma$  un sous-groupe fini d'ordre  $n$  de  $H$ . On dira que  $x \in \hat{\mathbb{C}}$  est un *pôle* de  $\Gamma$  s'il existe un élément  $f$  de  $\Gamma$ , distinct de l'identité, tel que  $f(x) = x$ .

a) Montrer que l'ensemble des pôles  $\mathcal{P}$  de  $\Gamma$  est un  $\Gamma$ -ensemble. ( $x \in \Gamma$  opère sur  $\mathcal{P}$ )

b) Soit  $L_x$  et  $H_x$  l'orbite et le stabilisateur de  $x$ , pôle de  $\Gamma$  et  $\eta_x$  et  $\nu_x$  leurs cardinaux. Etablir la relation:

$$2 - \frac{2}{n} = \sum_{L_x} \left(1 - \frac{1}{\nu_x}\right).$$

On pourra introduire le nombre de couples  $(f, x)$  où  $f$  est un élément de  $\Gamma$ , distinct de l'identité et où  $x$  est un pôle de  $f$ . En déduire qu'il ne peut y avoir que deux ou trois orbites.

**Question 4.** — Montrer que s'il n'existe que deux orbites,  $\Gamma$  est un groupe cyclique d'ordre  $n$ .

**Question 5.** — On suppose qu'il existe trois orbites dans le  $\Gamma$ -ensemble  $\mathcal{P}$ . On notera  $\nu_1, \nu_2, \nu_3$  les cardinaux des stabilisateurs avec  $\nu_1 \leq \nu_2 \leq \nu_3$ .

a) Montrer que  $\nu_1 = 2$  et  $2 \leq \nu_2 < 4$ .

b) Si  $\nu_2 = 2$ , montrer que  $\Gamma$  est le groupe diédral  $D_{\nu_3}$  des isométries planes qui laissent globalement invariant un polygone régulier de  $\nu_3$  sommets.

c) Si  $\nu_2 = 3$ , montrer que  $n = 6k$  avec  $k \geq 2$  et  $\nu_3 = \frac{6k}{k+2}$ , en déduire que  $n$  ne peut prendre que trois valeurs.

# Question d) TO

7

Il existe  $J \triangleleft N$ ,  $J$  sous-groupe d'ordre 5  $\Rightarrow J$  cyclique  $J = \langle \sigma \rangle$

Donc  $\sigma$  est d'ordre 5 dans  $J_5$ , donc  $\sigma =$  permutation circulaire.

Ainsi,  $\exists$  ordre 5  $\sigma = (1, 2, 3, 4, 5)$   $J = \langle \sigma \rangle \subset J_5$ .

$$\tau = (1, 2, 3) \Rightarrow \tau J \tau^{-1} \neq J$$

$J =$  ensemble des 5-sous-groupes de Sylow de  $N$

$$\left. \begin{array}{l} n = \# J \\ n \equiv 1 \pmod{5} \\ \text{et } n \mid \# N \mid 60 \Rightarrow n \mid 60 \end{array} \right\} \Rightarrow n = 6$$

$J_1, J_2, J_3, J_4, J_5$  sont disjoints deux à deux

Donc  $N$  contient  $4 \times 6 = 24$  éléments d'ordre 5. Comme  $\# N = 5, 10, 15, 30, 60$  (cf. (\*)  $\Rightarrow 5 \mid \# N$ , et  $2 \mid \# N \mid 60$ )  
ou 60, on aura nécessairement :

$$\# N = 30 \text{ ou } 60$$

Supposons, par l'absurde, que  $\# N = 30$ . Alors  $N$  contient 6 éléments d'ordre ~~différents de 5~~ 6 ; notons les  $1, a, b, c, d, e$ .

$$N \text{ opère sur } \{1, 2, 3, 4, 5\} \quad \# N = \#(\text{orb } 1) (\# H_1) = 5 \cdot \# H_1 \quad (*)$$

$$\text{où } H_1 = \{g \in N \mid g(1) = 1\}$$

$$\# N = 30 \text{ et } (*) \Rightarrow \# H_1 = 6$$

Alors je dis (il dit) que  $H_1 = \{1, a, b, c, d, e\}$ . En effet, sinon  $\exists$  el. d'ordre 5 dans  $H_1 \Rightarrow \exists h \in J_h \subset H_1$  absurde car  $\left\{ \begin{array}{l} \# J_h = 5 \\ \# H_1 = 6 \end{array} \right.$

$$\text{Donc } H_1 = \{1, a, b, c, d, e\}$$

On peut refaire ce développement (à partir de (\*)). On obtient :

$$\left. \begin{array}{l} H_1 = H_2 = H_3 = H_4 = H_5 = \{1, a, b, c, d, e\} \\ \text{ce qui est absurde, puisque } H_1 \cap \dots \cap H_5 = \{\text{Id}\} \end{array} \right\} \Rightarrow \{1, a, b, c, d, e\} = \{1\} \text{ absurde}$$

Conclusion :  $A_5$  est simple

- ① Déterminer : tous les sous anneaux de  $\mathbb{Z}$ , les systèmes libres, générateurs minimaux, toutes les bases.  
- Même questions pour  $\mathbb{Z}/p\mathbb{Z}$  considéré comme  $\mathbb{Z}$ -module

x ② Soient  $A$  un anneau,  $M$  un  $A$ -module. ( $A$  commutatif)

- Déterminer  $\text{Hom}_A(A, M)$

- Soit  $M^* = \text{Hom}_A(M, A)$

Muni  $M^*$  d'une structure de  $A$ -module

Montrer qu'il existe une application naturelle  $M \rightarrow M^{**}$ , en général ni injective ni surjective.

Déterminer  $(\mathbb{Z}/p\mathbb{Z})^*$ ,  $\mathbb{Z}/p\mathbb{Z}$  étant considéré comme un  $\mathbb{Z}$ -module

(resp. comme  $\mathbb{Z}/q\mathbb{Z}$ -module où  $q$  divise  $p$ )

- Déterminer  $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$  (considérer  $d = \text{pgcd}(m, n)$ )

<sup>(\*)</sup> - Si  $M$  est simplement un  $A$ -module à gauche ( $A$  non commutatif),  $M^*$  est un  $A$ -module à droite

- ③ Exemple Le  $A$ -module à gauche admettant les bases de cardinaux distincts  $E = \mathbb{C}[X]$

$A = \mathcal{L}(E, E)$  (applications  $\mathbb{C}$ -linéaires)

- Montrer que  $A$  est muni d'une structure de  $A$ -module à gauche, libre de rang 1.

- Soient  $\alpha, \beta \in A$  définis par

$$\alpha(P)(X^2) = \frac{P(X) + P(-X)}{2}$$

$$X \cdot \beta(P)(X^2) = \frac{P(X) - P(-X)}{2}$$

montrer que  $\{\alpha, \beta\}$  est une base de  $A$

Hint  $P \xrightarrow{u} P(X^2)$  satisfait  $\bar{\alpha} : \text{Id} = u \circ \alpha + v \circ \beta$

$$P \xrightarrow{v} X P(X^2)$$

$$\alpha \circ u = \text{Id}, \quad \beta \circ u = 0$$

$$\alpha \circ v = 0, \quad \beta \circ v = \text{Id}$$



on dit que  $I$  est irréductible si on a, c'est-à-dire si  $\{I = J \cap K \Rightarrow J = I \text{ ou } J = K\}$  2

x (4) Définition  $I$  idéal d'un anneau  $A$  (commutatif)

$I$  est irréductible si:  $\exists J, K$  idéaux de  $A$

$$I \not\subseteq J, I \not\subseteq K \text{ et } I = J \cap K$$

$$(a) \{0\} = \bigcap \{I \mid I \text{ idéal irréductible de } A\}$$

considérer  $a \neq 0$  et  $\mathcal{O} = \{I \text{ idéal} \mid a \notin I\}$

$$(b) I = \bigcap \{I' \supset I \mid I' \text{ irréductible}\}$$

(c) Déterminer les idéaux irréductibles de  $\mathbb{Z}$

d)  $I$  maximal  $\Rightarrow I$  premier  $\Rightarrow I$  irréductible

x (5) Soit  $A$  un anneau commutatif,  $M$  un  $A$ -module libre muni d'une base  $\{x_1, \dots, x_n\}$

a) Soit  $\mathcal{P}$  un idéal maximal de  $A$ . Montrer que  $M/\mathcal{P}M$  est un espace vectoriel sur  $A/\mathcal{P}$ .

b) Montrer que les classes des  $x_i$  dans  $M/\mathcal{P}M$  forment une base de cet espace vectoriel. En déduire que  $n$  ne dépend pas de la base choisie.

N.B. Si  $I$  est un idéal de  $A$ ,  $M$  un  $A$ -module  $I \cdot M$  désigne l'ensemble des sommes finies  $\sum \lambda_i x_i$ ,  $\lambda_i \in I, x_i \in M$ . On montrera que  $I \cdot M$  est un  $A$ -module de  $M$ , et dans (a) que  $\mathcal{P}M$  est l'ensemble des  $\mu_1 x_1 + \dots + \mu_n x_n$ ,  $\mu_i \in \mathcal{P}$ , cette écriture étant unique.

Cet exercice montre que le phénomène de l'exo (3) n'a lieu que pour des anneaux non commutatifs.

x (6) Soit  $A$  un anneau  $A^n$  est un  $A$ -module à gauche

$$\text{Hom}_A(A^n, A) \cong A^n$$

Soit  $u: M \rightarrow N$  une application  $A$ -linéaire

$${}^t u: N^* \rightarrow M^* \quad {}^t u(n^*) = n^* \circ u$$

Montrer  $u$  surjective  $\Rightarrow {}^t u$  injective  
et par des contre-exemples:

$${}^t u \text{ injective} \not\Rightarrow u \text{ surjective}$$

$$u \text{ injective} \not\Rightarrow {}^t u \text{ surjective}$$

- ④  $I$  est réductible ssi  $\exists J, K$  idéaux de  $A$   $I \subsetneq J$  et  $I \subsetneq K$  et  $I = J \cap K$   
 $I$  irréductible sinon, c-à-d ssi  $I = J \cap K \Rightarrow J = I$  ou  $J = K$ .

a)  $\{0\} = \text{intersection des idéaux irréductibles de } A$ .

Soit  $a \neq 0$ ,  $a \in A$ . Considérons  $\mathcal{J} = \{I \subset A \mid I \text{ idéal et } a \notin I\}$

Exhibons un élément irréductible dans  $\mathcal{J}$ .

Pour cela, remarquons que :

\* ~~Tout idéal maximal est irréductible.~~

\*  $\mathcal{J}$  possède au moins 1 él. maximal.

En effet, d'après la définition de  $\mathcal{J}$ ,  $\mathcal{J}$  est ordonné

(pour l'inclusion) et inductif (car si  $(I_\lambda)_{\lambda \in \Lambda} \subset \mathcal{J}$  totalement ordonné, alors

$I = \bigcup_{\lambda \in \Lambda} I_\lambda$  est un idéal ne contenant pas  $a$ . Donc  $I \in \mathcal{J}$  et  $I$  majore la partie  $(I_\lambda)_{\lambda \in \Lambda}$ . Donc  $\mathcal{J}$  possède au moins un élément maximal

noté :  $I$

Montrons que  $I$ , maximal dans  $\mathcal{J}$ , est irréductible.

Si  $J, K$  idéaux /  $\begin{cases} I \subsetneq J \\ I \subsetneq K \end{cases}$  et  $I = J \cap K$  alors  $J \notin \mathcal{J} \Rightarrow a \in J$   
 $\Rightarrow a \in K$

donc  $a \in J \cap K = I$ , ce qui est absurde.

Donc  $I$  est irréductible.

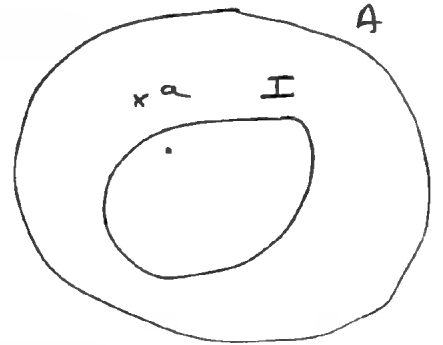
CPFD

On a montré que  $\forall a \in A$   $a \neq 0$   $\exists I$  irréductible /  $a \notin I$

d'où, en notant  $L = \{\text{intersection des idéaux irréductibles de } A\}$ ,

on a  $a \in A$   $a \neq 0 \Rightarrow a \notin L$  d'où  $\bigcup_A \{0\} \subset L \Leftrightarrow L \subset \{0\}$ .

d'où  $L = \{0\}$



$$b) \quad I = \bigcap \{ I' \supset I \mid I' \text{ irréductible} \} \quad (b)$$

Préliminaire:

**I** Quels sont les idéaux de  $A/I$ ? Ce sont les  $I'/I$  où  $I'$  est un idéal de  $A$  contenant  $I$ .

$$A \xrightarrow{\varphi} A/I \quad \varphi = \text{homomorphisme d'anneaux.}$$

$$\mathcal{I}_A^I = \{ \text{idéaux de } A \text{ contenant } I \} \xrightarrow{\varphi} \{ \text{idéaux de } A/I \} = \mathcal{I}_{A/I}$$

$$\mathcal{I}_A^I = \varphi^{-1}(\mathcal{I}_{A/I}) \quad \longleftarrow \quad \mathcal{I}_{A/I}$$

$$I' \xrightarrow{\quad} \varphi(I') = I'/I$$

car  $\varphi$  surjective.

On a  $\varphi(\varphi^{-1}(\mathcal{I}_{A/I})) = \mathcal{I}_{A/I}$ . On a toujours  $\varphi^{-1}(\varphi(I')) \supset I'$

$$\text{Si } I \subset I', \quad x \in \varphi^{-1}(\varphi(I')) \quad \varphi(x) \in \varphi(I')$$

$$\exists y \in I' \quad \varphi(x) = \varphi(y) \Rightarrow x - y \in I \subset I' \Rightarrow x \in I'$$

$$\text{d'où } \varphi^{-1}(\varphi(I')) = I'.$$

Ainsi  $\varphi \circ \varphi^{-1} = \varphi^{-1} \circ \varphi = \text{Id}$ , donc  $\varphi$  est bijective de  $\mathcal{I}_A^I$  sur  $\mathcal{I}_{A/I}$

**II** Prop.  $\parallel I'/I$  idéal irréductible de  $A/I \iff I'$  est un idéal irréductible de  $A$ , contenant  $I$ .

On a:

$$\cancel{I'/I} \quad \frac{J'}{I} \cap \frac{K'}{I} = \frac{J' \cap K'}{I} \quad (\text{II}')$$

$$I'/I \text{ irréductible} \iff \left\{ I'/I = \frac{J'}{I} \cap \frac{K'}{I} \Rightarrow \frac{I'}{I} = \frac{J'}{I} \text{ ou } \frac{I'}{I} = \frac{K'}{I} \right\}$$

$$\iff \left\{ I' = J' \cap K' \Rightarrow I' = J' \text{ ou } I' = K' \right\}$$

$$\iff I' \text{ irréductible.}$$

Montrons (b)

$$\{0\} = \bigcap \{ I'/I \text{ irréductible} \} \iff I = \bigcap \{ I' \supset I \mid I' \text{ irréductible} \}$$

$$\bigcap \{ I' \text{ irréductibles} \}$$

CQFD

Remarques :  $I \subset A$  idéal,  $A/I$ , Soit  $\{J_\lambda\}_{\lambda \in \Lambda}$  une famille d'idéaux de  $A$  tels que  $I \subset J_\lambda$ . Considérons l'idéal  $\bigcap \{J_\lambda/I\}_{\lambda \in \Lambda}$ . On a :  $\bigcap (J_\lambda/I)_{\lambda \in \Lambda} = \frac{\bigcap (J_\lambda)_{\lambda \in \Lambda}}{I}$

Si  $x \in \bigcap_{\lambda \in \Lambda} (J_\lambda/I) \Leftrightarrow \forall \lambda \in \Lambda, x \in J_\lambda/I \Leftrightarrow \forall \lambda \in \Lambda, x \in J_\lambda$ .

### c) Idéaux irréductibles de $\mathbb{Z}$

Les idéaux irréductibles de  $\mathbb{Z}$  sont les  $n\mathbb{Z}$  qui vérifient (1)

$$n\mathbb{Z} = x\mathbb{Z} \cap y\mathbb{Z} \Rightarrow x\mathbb{Z} = n\mathbb{Z} \text{ ou } y\mathbb{Z} = n\mathbb{Z} \quad (1)$$

Montrons que :

$$\text{On a } \left| n\mathbb{Z} \text{ irréductible} \Leftrightarrow n=0 \text{ ou } n=p^k \text{ où } p \in \mathcal{P} \right.$$

( $\Leftarrow$ ) • Si  $n=0$ ,  $0\mathbb{Z} = J \cap K = x\mathbb{Z} \cap y\mathbb{Z} \Rightarrow xy \in 0\mathbb{Z} \Rightarrow xy=0$   
d'où  $x=0$  ou  $y=0$

• Si  $n=p^k$  où  $k \in \mathbb{N}$  et  $p \in \mathcal{P}$  ( $p > 0$ ), considérons

$$p^k\mathbb{Z} = x\mathbb{Z} \cap y\mathbb{Z}$$

$$\begin{cases} x \mid p^k \Rightarrow \exists \alpha \in \mathbb{N} / x = p^\alpha \\ y \nmid p^k \Rightarrow \exists \beta \in \mathbb{N} / y = p^\beta \end{cases}$$

$$\text{d'où } p^k\mathbb{Z} = p^\alpha\mathbb{Z} \cap p^\beta\mathbb{Z}$$

Comme  $p^\alpha \mathbb{Z} \cap p^\beta \mathbb{Z} = \mu(p^\alpha, p^\beta) \mathbb{Z} = p^{\sup(\alpha, \beta)} \mathbb{Z}$ , on en déduit que  $x = p^k$  ou  $y = p^k$ .

( $\Rightarrow$ ) Inversement, soit  $n \in \mathbb{Z}$  irréductible et tel que  $n \neq 0$ . Ou bien  $n = 1$ , et c'est terminé. Ou bien  $n \neq 1$ . Alors  $n$  possède au moins 1 ~~facteur~~ diviseur  $p$  premier. Montrons que  $n = p^k$  où  $k \in \mathbb{N}$ .

$$n = p^k q \text{ où } \Delta(p, q) = 1, \text{ et donc } \mu(p^k, q) = \frac{n}{p^k}$$

$$\text{d'où : } n \mathbb{Z} = p^k \mathbb{Z} \cap q \mathbb{Z} \Rightarrow n = p^k \text{ ou } n = q$$

$n \neq q$  car autrement  $n = p^k \cdot n \Rightarrow p^k = 1 \Rightarrow k = 0$ , absurde car  $p \mid n$ .

Donc  $n = p^k$ .

CQFD

(Remarque : d'habitude, on exclut l'anneau  $A$  pour l'irréductibilité)

d)  $I \text{ maximal} \Rightarrow I \text{ premier}$

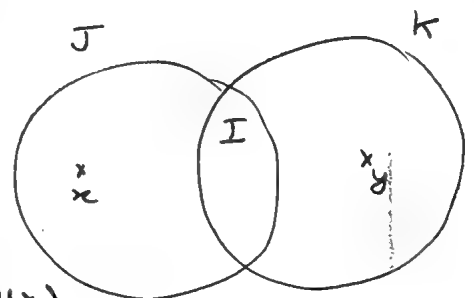
fait sur le Quercy, Th 1. p 59.

$I \text{ premier} \Rightarrow I \text{ irréductible}$

Par l'absurde, si  $I$  premier et  $I$  ~~irréductible~~ réductible,

alors  $\exists J, K / I = J \cap K$  et  $I \subsetneq J$

$$\begin{matrix} \mathbb{K} \\ I \subsetneq K \end{matrix}$$



Soit  $x \in J \setminus I$  et  $y \in K \setminus I$ .

On a  $xy \in J \cap K$  (car  $J$  et  $K$  sont des idéaux)

Donc  $xy \in I \Rightarrow x \in I$  ou  $y \in I$ , ce qui est absurde.

Remarque:  $IJ = \left\{ \sum_{i=1}^n x_i y_i \mid x_i \in I \text{ et } y_i \in J, n \in \mathbb{N} \right\}$

- (2x0)
- 1)  $IJ$  est un idéal de  $A$ , c'est l'idéal engendré par  $\{xy \mid x \in I \text{ et } y \in J\}$
  - 2)  $IJ \subset I \cap J$ . Montrer qu'on peut avoir  $IJ \subsetneq I \cap J$
  - 3) Si  $\mathcal{P}$  est un idéal premier,  $I \cap J \subset \mathcal{P} \Rightarrow I \subset \mathcal{P} \text{ ou } J \subset \mathcal{P}$ .
  - 4)  $\mathcal{P} \subset \mathcal{P}_1 \cup \dots \cup \mathcal{P}_n$  avec  $\mathcal{P}_i$  premiers  $\Rightarrow \exists i \mid \mathcal{P} \subset \mathcal{P}_i$

3)  $(m\mathbb{Z})(n\mathbb{Z}) = mn\mathbb{Z}$  puisque  $\forall x \in (m\mathbb{Z})(n\mathbb{Z})$

$$x = \sum m x_i n y_i \in mn\mathbb{Z}$$

d'où  $(m\mathbb{Z})(n\mathbb{Z}) \subset mn\mathbb{Z}$  et  $(m\mathbb{Z})(n\mathbb{Z})$  contient  $mn$ , d'où =.

De plus  $(m\mathbb{Z})(n\mathbb{Z}) \subset m\mathbb{Z} \cap n\mathbb{Z}$ ssi  $\Delta(m,n) \neq 1$ .

4)

$n=2$

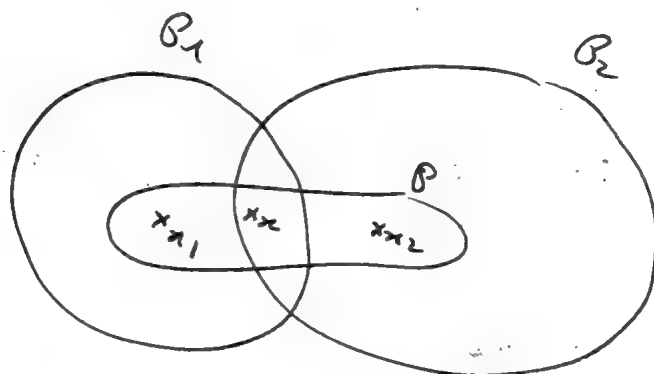
Supposons, par l'absurde, que

$$\begin{cases} \mathcal{P} \not\subset \mathcal{P}_1 \Rightarrow \exists x_2 \in \mathcal{P} \setminus \mathcal{P}_1 & x_2 \in \mathcal{P}_2 \\ \mathcal{P} \not\subset \mathcal{P}_2 \Rightarrow \exists x_1 \in \mathcal{P} \setminus \mathcal{P}_2 & x_1 \in \mathcal{P}_1 \end{cases}$$

$$x = x_1 + x_2 \in \mathcal{P} \subset \mathcal{P}_1 \cup \mathcal{P}_2$$

si  $x \in \mathcal{P}_1$ , on a  $x_2 \in \mathcal{P}_1$  absurde

si  $x \in \mathcal{P}_2$ , on a  $x_1 \in \mathcal{P}_2$  absurde



NB: on n'a pas utilisé le fait que  $\mathcal{P}_1$  et  $\mathcal{P}_2$  étaient premiers:

En ||  $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P} \exists$  idéaux (qcg)  $\mathcal{P} \subset \mathcal{P}_1 \cup \mathcal{P}_2 \Rightarrow \mathcal{P} \subset \mathcal{P}_1 \text{ ou } \mathcal{P} \subset \mathcal{P}_2$ .

n quelconque: récurrence. Le théorème est vrai pour  $n-1$  idéaux premiers. ( $n \geq 2$ )

\* Si  $\mathcal{P} \subset \mathcal{P}_1 \cup \dots \cup \mathcal{P}_{i-1} \cup \mathcal{P}_{i+1} \cup \dots \cup \mathcal{P}_n$ , on aurait  $\mathcal{P} \subset \mathcal{P}_k$  (hyp. réc.)

\* Si l'on a  $\mathcal{P} \not\subset \mathcal{P}_1 \cup \dots \cup \mathcal{P}_{i-1} \cup \mathcal{P}_{i+1} \cup \dots \cup \mathcal{P}_n \quad \forall i \in [1, n]$ , on a:

on a:

Il existe  $y_i \in \mathcal{P}$  et  $y_i \notin \mathcal{P}_1 \cup \dots \cup \mathcal{P}_{i-1} \cup \mathcal{P}_{i+1} \cup \dots \cup \mathcal{P}_n \Rightarrow y_i \in \mathcal{P}_i$

donc  $y_i \in \mathcal{P}_i$  et  $y_i \notin \mathcal{P}_j$  pour  $j \neq i$ . (où  $y_i \in \mathcal{P}$ )

$$\text{si } \forall i \ x_i \notin \mathcal{P}_i \quad \forall j \neq i \ x_j \in \mathcal{P}_i \quad x_1 + \dots + x_i + \dots + x_n \in \mathcal{P}_i$$

On prend  $x_i = y_1 \dots y_{i-1} y_{i+1} \dots y_n \in \mathcal{P}_j \quad \forall j \neq i$   
 $\notin \mathcal{P}_i$  car  $\mathcal{P}_i$  premier  
 ( $x_i \in \mathcal{P}_i \Rightarrow \exists k \leq i \ y_k \in \mathcal{P}_i$  absurde)

Ainsi  $x_i \in \mathcal{P} \quad \forall i$  et  $x_1 + \dots + x_n \notin \mathcal{P}_1 \cup \dots \cup \mathcal{P}_n$ .

C'est absurde.

Dans tous les cas  $\exists i \ / \ \mathcal{P} \subset \mathcal{P}_1 \cup \dots \cup \mathcal{P}_i \cup \mathcal{P}_i \cup \dots \cup \mathcal{P}_n$

CQFD

Exo

Soit  $A$  un anneau commutatif unitaire.

$$\text{Nil}(A) = \{x \in A \ / \ \exists n \in \mathbb{N} \ x^n = 0\}$$

C'est le nilradical de l'anneau  $A$ .

1° Déterminer  $\text{Nil}(A)$  dans chacun des cas :  $A = K[X]/(X^n)$  où  $K = \text{corps}$  ;  $A = \mathbb{Z}/p^k\mathbb{Z}$  ;  $A = \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \dots \times p_s^{k_s}\mathbb{Z}$

2° Montrer que  $\text{Nil}(A)$  est un idéal de  $A$ .

$$3^\circ \text{ Montrer } \text{Nil}(A) = \bigcap_{\substack{\mathcal{P} \text{ idéal} \\ \text{premier}}} \mathcal{P} \quad (\text{cf. Zuercher})$$

$$\begin{aligned} 1^\circ \ A = \mathbb{Z}/p^k\mathbb{Z} \quad x \in \text{Nil}(A) &\Leftrightarrow \exists n \in \mathbb{N} \ / \ p^k \mid x^n \\ &\Leftrightarrow p \mid x \\ &\Leftrightarrow \exists \lambda \in \mathbb{Z} \ / \ x = \lambda p = p\lambda \end{aligned}$$

$$\text{Nil}(\mathbb{Z}/p^k\mathbb{Z}) = p \mathbb{Z}/p^k\mathbb{Z}$$

On montre, de même, que  $\text{Nil } A = X \ K[X]/(X^n)$

mandi  
15 janvier 80 : Théorème Chinois.

$\mathfrak{a}_i$  idéal de  $A$ . Je dis que  $\mathfrak{a}_1$  et  $\mathfrak{a}_2$  sont étrangers (premiers entre eux) si  $\mathfrak{a}_1 + \mathfrak{a}_2 = A$ .

(On suppose  $A$  anneau commutatif et unitaire)

1) Montrer que  $\mathfrak{a}_1 + \mathfrak{a}_2 = A \iff \mathfrak{a}_1 \cdot \mathfrak{a}_2 = \mathfrak{a}_1 \cap \mathfrak{a}_2$ . Envisager la réciproque.

2) Montrer que  $A/\mathfrak{a}_1 \times A/\mathfrak{a}_2 \cong A/\mathfrak{a}_1 \cap \mathfrak{a}_2$  (si  $\mathfrak{a}_1 + \mathfrak{a}_2 = A$ )

3) généralisation:  $\mathfrak{a}_1, \dots, \mathfrak{a}_n$  deux à deux étrangers. Montrer qu'alors

a)  $\mathfrak{a}_1 + \mathfrak{a}_2 + \dots + \mathfrak{a}_n = A$  et  $\mathfrak{a}_1 \dots \mathfrak{a}_n = \mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_n$

b)  $A/\mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_n \cong A/\mathfrak{a}_1 \times \dots \times A/\mathfrak{a}_n$

c)  $A/\mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_n \longrightarrow A/\mathfrak{a}_1 \times \dots \times A/\mathfrak{a}_n$   
 $\pi \longmapsto (\pi_1, \dots, \pi_n)$  est un isomorphisme de groupes.

1) Si  $\mathfrak{a}_1 + \mathfrak{a}_2 = A$ , montrons que  $\mathfrak{a}_1 \cap \mathfrak{a}_2 \subset \mathfrak{a}_1 \cdot \mathfrak{a}_2$ .

$\forall x \in \mathfrak{a}_1 \cap \mathfrak{a}_2 \quad 1 = x_1 + x_2 \quad x_1 \in \mathfrak{a}_1 \quad x_2 \in \mathfrak{a}_2$

d'où  $x = \underbrace{x x_1}_{\in \mathfrak{a}_1 \mathfrak{a}_2} + \underbrace{x x_2}_{\in \mathfrak{a}_1 \mathfrak{a}_2} \in \mathfrak{a}_1 \cdot \mathfrak{a}_2$ .

Exemple:  $n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z} \iff n\mathbb{Z} \cap m\mathbb{Z} = nm\mathbb{Z} = (n\mathbb{Z}) \cdot (m\mathbb{Z})$

On a l'équivalence dans n'importe quel anneau principal, et en particulier dans  $K[X]$  où  $K$  est un corps.

⚠ Il existe des anneaux  $A$  tels que  $\mathfrak{a}_1 \cdot \mathfrak{a}_2 = \mathfrak{a}_1 \cap \mathfrak{a}_2$  et pourtant  $\mathfrak{a}_1 + \mathfrak{a}_2 \neq A$ .

Prendons  $A = K[X, Y]$ ,  $\mathfrak{a}_1 = (X)$  et  $\mathfrak{a}_2 = (Y)$ .

$$\begin{cases} \mathfrak{a}_1 \cap \mathfrak{a}_2 = (XY) & \text{car } \mathfrak{a}_1 = \{P / P(0, Y) = 0\}; \mathfrak{a}_2 = \{Q / Q(X, 0) = 0\} \\ \mathfrak{a}_1 \mathfrak{a}_2 = (XY) \end{cases}$$

donc  $\mathfrak{a}_1 \mathfrak{a}_2 = \mathfrak{a}_1 \cap \mathfrak{a}_2$



Et pourtant  $a_1 + a_2 = \{pX + qY \mid p, q \in K[X, Y]\} \neq d$  car

$1 \notin a_1 + a_2$  (cf.  $pX + qY = 1 \Rightarrow 0 = 1$  absurde).

[NB : autre façon de conclure :  $a_1 + a_2 = \{p \mid p(0,0) = 0\} \Rightarrow 1 \notin a_1 + a_2$ ]

2)

La suite :  $0 \rightarrow a_1 \cap a_2 \xrightarrow{i} A \xrightarrow{\beta} A/a_1 \times A/a_2$  est exacte (de groupes +)  
 $x \mapsto (\bar{x}_1, \bar{x}_2)$

Tout le problème consiste à montrer que  $\beta$  est surjective.

Je pose  $1 = x_1 + x_2$ .

Résolvons 
$$\begin{cases} y = y_1 \pmod{a_1} \\ y = y_2 \pmod{a_2} \end{cases} \quad (1)$$

On a :  $(\bar{x}_2, \bar{x}_2) = (1, \bar{0})$

$(\bar{x}_1, \bar{x}_1) = (\bar{0}, 1)$

On prend  ~~$y = y_1(\bar{x}_2) + y_2(\bar{x}_1)$~~

$y = y_1 x_2 + y_2 x_1$  - On a bien  $(\bar{y}, \bar{y}) = (\bar{y}_1, \bar{y}_2)$ .

ce qui donne 1 solution de (1).

$\forall y'$  solution,  $y - y' \in a_1 \cap a_2$

Application : Dans  $\mathbb{Z}$  
$$\begin{cases} y \equiv y_1 \pmod{a_1} \\ y \equiv y_2 \pmod{a_2} \end{cases} \quad \text{où } \Delta(a_1, a_2) = 1$$

admet 1 solution et 1 seule modulo le ppcm  $(a_1, a_2)$ .

C'est la classe de  $y_1 a_2 v + y_2 a_1 u$  où  $a_2 u + a_1 v = 1$

3) Pour n idéaux  $a_1, \dots, a_n$  tels que  $a_i + a_j = A \quad \forall i \neq j$ .

$$\begin{cases} 1 = x_{12} + x_2 \\ 1 = x_{13} + x_3 \\ \vdots \\ 1 = x_{1n} + x_n \end{cases} \quad \begin{aligned} 1 &= \prod_{j=2}^n (x_{1j} + x_j) \\ 1 &= \underbrace{x_1^n}_{\in a_1} + x_2 \dots x_n \in a_1 + a_2 \dots a_n \end{aligned}$$



$$x = 642 + \lambda \text{ppcm}(11, 9, 5) \quad \lambda \in \mathbb{Z}$$

le plus petit  $x$  positif est  $x = 642 - 495 = 147$

### Exercice

Soient:

$$\mathfrak{r}(A) = \bigcap \{ \mathfrak{m} \in A / \mathfrak{m} \text{ idéal maximal} \} = \text{radical de } A$$

$$A^* = \{ x \in A / \exists y \in A \quad xy = 1 \} \text{ est un groupe pour } \cdot$$

$$(\mathbb{Z}^* = \{ \pm 1 \} ; (\mathbb{R}[X])^* = \mathbb{R}^*)$$

$$\text{Montrer que } x \in \mathfrak{r}(A) \Leftrightarrow \forall y \in A \quad 1 - xy \in A^*$$

Solution:

$$\begin{aligned} (\Leftarrow) \quad x \notin \mathfrak{r}(A) &\Leftrightarrow \exists \mathfrak{m} \text{ idéal maximal} / x \notin \mathfrak{m} \\ &\Leftrightarrow xy = 1 + m \text{ où } m \in \mathfrak{m} \\ &\Leftrightarrow 1 - xy \in \mathfrak{m} \text{ maximal} \Rightarrow 1 - xy \notin A^* \text{ (sinon } \mathfrak{m} = A) \end{aligned}$$

$$(\Rightarrow) \text{ Supposons que } x \in \mathfrak{r}(A) \text{ et que } 1 - xy \notin A^*.$$

Alors  $\exists \mathfrak{m}$  idéal maximal contenant  $1 - xy$ .

$$\left. \begin{array}{l} 1 - xy \in \mathfrak{m} \\ \text{et } x \in \mathfrak{m} \end{array} \right\} \Rightarrow 1 \in \mathfrak{m} \Rightarrow \mathfrak{m} = A, \text{ absurde.}$$

Donc  $1 - xy \in A^*$ .

Remarque:  $\mathfrak{r}(\mathbb{Z}) = \{0\}$  car  $\mathfrak{r}(\mathbb{Z}) = \bigcap_{p \in \mathcal{P}} p\mathbb{Z}$  et  $\mathcal{P}$  est infini.

Essayons de trouver un exemple de  $\mathfrak{r}(A)$  non banal. Pour cela, considérons le corps des fractions rationnelles  $K(X) = \{ \frac{P}{Q} / P, Q \in K[X] \}$

$$\text{Soit } K(X)_0 = \{ \frac{P}{Q} \in K(X) / Q(0) \neq 0 \} = A$$

On a  $P(0) \neq 0 \Leftrightarrow P/Q$  inversible dans  $K(X)$ .

Soit  $\mathcal{M} = \{ P/Q \in A \mid P(0) = 0 \}$ . C'est un idéal maximal (car si

$\frac{P'}{Q'} \notin \mathcal{M}$ ,  $\mathcal{M} + (\frac{P'}{Q'}) = K(X)$ . car  $P'(0) \neq 0 \Rightarrow \frac{P'}{Q'}$  inversible dans  $K(X)$ ).

Il est clair (ou obscur) que  $\mathcal{M}(A) = \mathcal{M}$ .

En effet, tout idéal différent de  $A$  est dans  $\mathcal{M}$  (sinon ...).

Généralisation :

lundi 21 janvier

Théorème : Soit  $A$  un anneau. Les 2 conditions suivantes sont équivalentes :

- 1)  $A \setminus A^*$  est un idéal
- 2)  $A$  possède un seul idéal maximal

Définition : Un tel anneau est dit "anneau local".

(exo : l'anneau des séries entières convergentes est un anneau local)

2)  $\Rightarrow$  1)  $\mathcal{M}$  est l'idéal maximal de  $A$ .

$\forall x \notin \mathcal{M}$  on a  $x \in A \setminus A^*$ . Or, il existe un idéal maximal qui contient  $x \in A$ . Cela peut être que  $\mathcal{M} : x \in A \subset \mathcal{M} \Leftrightarrow x \notin A^*$

d'où  $\mathcal{M} = A \setminus A^*$

1)  $\Rightarrow$  2) Si  $\mathcal{I}$  est un idéal propre de  $A$ ,  $\mathcal{I} \subset A \setminus A^*$ . Donc si  $A \setminus A^*$  est un idéal, c'est forcément l'idéal maximal de  $A$ .

[cf : Soit  $\mathcal{J}$  un idéal maximal quelconque,  $\mathcal{J} \subset A \setminus A^* \Rightarrow \mathcal{J} = A \setminus A^*$ ]

CQFD

Exercice : Montrer que l'anneau  $\mathbb{Z}/p^n\mathbb{Z}$  est local.

Solution :  $A = \mathbb{Z}/p^n\mathbb{Z}$   $k \in \mathbb{Z}/p^n\mathbb{Z}$ . Cherchons  $A^*$ .

$$A^* = \{ k' \in A \mid \Delta(k', p^n) = 1 \}$$

Où  $k \in A^* \Leftrightarrow p \nmid k$  donc  $A \setminus A^* = p(\mathbb{Z}/p^n\mathbb{Z})$  est un idéal

(NB : même chose avec  $K[X]/(X^n)$ )

Exercice :  $K[[X]]$ , anneau des séries formelles, est un anneau local dont l'idéal maximal est  $XK[[X]]$ .

Solution :  $A \setminus A^* = XK[[X]]$  est un idéal.

cf :  $P \in A^* \Leftrightarrow P(0) \neq 0$ .

Anneaux des fractions : Soit  $A$  un anneau,

$S$  est une partie multiplicative si  $x, y \in S \Rightarrow xy \in S$ . Supposons que  $0 \notin S$  et considérons  $A \times S$  muni de la relation d'équivalence suivante :

$$(x, s) \sim (x', s') \Leftrightarrow s''xs' = x'ss'' \exists s'' \in S \\ \Leftrightarrow s''(xs' - x's) = 0 \quad s'' \in S.$$

(NB : Si  $A$  est intègre, on pourra supprimer  $s''$ )

Alors  $A_S = A \times S / \sim$  est un anneau.

En notant  $(\frac{x}{s}) = \frac{x}{s}$ , on pose  $\varphi : A \rightarrow A_S$   
 $x \mapsto \frac{x}{1}$  (NB : si  $1 \notin S$ ,  $\frac{0x}{s} = \frac{x}{1}$  bien connu)

$\varphi$  est un homomorphisme,  $\varphi(A) \subset A_S^*$  et  $\varphi$  est injective dès que  $A$  est intègre.

(Note sur  $s''$  : si  $sx = 0 \Rightarrow \varphi(s)\varphi(x) = 0$ . On veut que  $\varphi(s)$  soit inversible, et donc que  $\varphi(x) = 0 \Rightarrow \frac{x}{1} = \frac{0}{1} \Leftrightarrow x \cdot 1 = 0 \cdot 1 \Leftrightarrow x = 0$ . Ainsi, on veut que  $\varphi(s)\varphi(x) = 0 \Rightarrow sx = 0$ .)

Solution :

$\sim$  est d'équivalence : RST

$$\text{Si } (x_1, s_1) \sim (x_2, s_2) \Leftrightarrow s'_1(x_1s_2 - s_1x_2) = 0 \Rightarrow \begin{cases} s''s'_1s'_2(x_1s_2 - s_1x_2) = 0 \\ s''s'_1s''_2(x_2s_3 - s_2x_3) = 0 \end{cases}$$

$$s's''(x_1s_2s_3 - s_1s_2x_3) = 0$$

$$s's''s_2(x_1s_3 - s_1x_3) = 0$$

$\Downarrow$

$$(x_1, s_1) \sim (x_3, s_3) \text{ oui.}$$

(NB : Si l'on n'avait pas  $s''$ , on n'aurait pas pu conclure)

(NB : Si  $A$  était intègre, on aurait raisonné différemment)

\*  $A_S$  est un anneau: On pose :

$$(\overline{x, s}) + (\overline{x', s'}) = \overline{(x s' + x' s, s s')}$$

et

$$(\overline{x, s}) (\overline{x', s'}) = \overline{(x x', s s')}$$

Ces opérations sont bien définies : Prenons  $(\overline{x, s}) = (\overline{x_1, s_1})$ , c.-à-d.  
 $\exists s'' \neq 0, s''(s_1 s - x_1 s) = 0$

Alors a-t-on  $\overline{(x s' + x' s, s s')} = \overline{(x_1 s' + x' s_1, s_1 s s')}$  ?

oui, puisque  $s_1 s' (x s' + x' s) - s s' (x_1 s' + x' s_1) = s'^2 (s_1 x - s x_1) = 0$

d'où :  $s'' \alpha = s'^2 s'' (s_1 x - s x_1) = 0$ .

On fait de même pour la loi  $\cdot$ .

On vérifie, comme pour  $\mathbb{Q}$ , que  $(A_S, +, \cdot)$  est un anneau, unitaire d'élément unité  $\frac{s}{s}$  ( $\frac{1}{1}$  si  $1 \in S$ ), puisque

$$(\overline{s, s s}) (\overline{x', s'}) = \overline{(s x', s s s')} = \overline{(x', s')}$$

\*  $\varphi$  est un morphisme : oui, et  $[\varphi(s)]^{-1} = \left[ \frac{s}{1} \right]^{-1} = \frac{1}{s} \Rightarrow \varphi(A) \subset A_S^*$

\*  $\ker \varphi$  ?  $\ker \varphi = \{x \mid \exists s'' \in S \quad x s'' = 0\} \subset A$  (est un idéal de  $A$ )

Il est clair que  $\ker \varphi = \{0\}$  si  $A$  est intègre, et même si  $S$  ne contient pas de diviseurs de 0.

CQFD

Exemples : ① Si  $A$  est intègre, on prend  $S = A \setminus \{0\} = A^*$  et on construit le corps des fractions de  $A$  :  $K = A_S$  est un corps..

$$\varphi : A \hookrightarrow K \text{ homomorphisme inj. d'anneaux,}$$

d'existence d'un plongement ( $\varphi$  monomorphisme ~~inj~~ d'anneaux) de  $A$  dans un corps  $K$  équivaut au fait que  $A$  soit intègre.

② Si  $A$  non intègre, on peut toujours prendre  $S = A^*$ , ou  $S = \{\text{ensemble des non diviseurs de } 0\}$  (qui est une partie multiplicativement

$$s, s' \in S \quad s s' x = 0 \Rightarrow s' x = 0 \Rightarrow x = 0.)$$

Dans ce cas  $\varphi$  est injective, et  $A_S$  est alors appelé "anneau total des fractions de  $A$ ".

L'exemple ② est bien moins utilisable que ①.

③ Soit  $\mathbb{Z}$  et  $\mathbb{Q}$ . Posons  $S = \mathbb{Z} \setminus p\mathbb{Z}$ .  $S$  est multiplicatif dès que  $p$  est premier, car  $x, y \in S \Rightarrow xy \in S$  ( $p \nmid x$  et  $p \nmid y \Rightarrow p \nmid xy$ )

$\mathbb{Z}_S = \{ \frac{m}{n} / p \nmid n \text{ (p premier)} \}$  est considérée comme partie de  $\mathbb{Q}$ .

D'où l'exercice :

Exercices: 1)  $A$  intègre, pour toute partie multiplicative  $S$ , on a des injections  $A \xrightarrow{\varphi} A_S \hookrightarrow K$  et  $A_S = \{ \frac{x}{y} \in K / y \in S \}$

(après identification)

Par exemple  $K(X)_0 = \{ \frac{p}{q} / q(0) \neq 0 \}$  (ici  $S = \{ q / q(0) \neq 0 \}$ )

2) Si  $\mathcal{P}$  est un idéal premier, a) montrer que  $S = A \setminus \mathcal{P}$  est une partie multiplicative. Dans ce cas là, on note  $A_{\mathcal{P}} = A_S$ . b) Montrer que  $A_{\mathcal{P}}$  est un anneau local dont l'idéal maximal est  $\mathcal{P} A_{\mathcal{P}} = \{ \frac{x}{y} / x \in \mathcal{P} \text{ et } y \notin \mathcal{P} \}$

dimanche 27 (Sup.) TDS

⑥ Anneau comm. unit.  $A^n$  est un  $A$ -module.

~~Note: Si  $A = \frac{M}{A}$  module à gauche, alors  $M$~~

\*  $\text{Hom}_A(A^n, A) \cong A^n$

Soit  $\beta \in \text{Hom}_A(A^n, A)$ ,  $\forall x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in A^n$   $\beta(x) = \sum_{i=1}^n x_i \beta(e_i)$  où  $e_i = \begin{pmatrix} 0 \\ \vdots \\ 1 \end{pmatrix}$  i-ème

Considérons

$$\begin{aligned} \varphi: \text{Hom}_A(A^n, A) &\longrightarrow A^n \\ \beta &\longmapsto \begin{pmatrix} \beta(e_1) \\ \vdots \\ \beta(e_n) \end{pmatrix} \end{aligned}$$

$\varphi$  est bijective, et c'est un homomorphisme d'anneaux de  $A$ -modules, puisque

$$\begin{cases} \varphi(\beta + \gamma) = \varphi(\beta) + \varphi(\gamma) \\ \varphi(\lambda \beta) = \begin{pmatrix} \lambda \beta(e_1) \\ \vdots \\ \lambda \beta(e_n) \end{pmatrix} = \lambda \varphi(\beta) \end{cases} \quad \forall \lambda \in A$$

\* \*  $M \xrightarrow{u} N$

$M^* \xleftarrow{t_u} N^*$

$t_u(n^*) = n^* \circ u$

(càd : on définit  $t_u$  par dualité, en posant  $\langle t_u(n^*), m \rangle = \langle n^*, u(m) \rangle$ )

Plus  $u$  surjective  $\Rightarrow t_u$  injective

C'est simple. Il suffit d'écrire que  $t_u(n^*) = t_u(k^*) \Leftrightarrow n^* \circ u = k^* \circ u$  c'est-à-dire  $n^*(u(m)) = k^*(u(m)) \quad \forall m \in M$ .

Si  $u$  est surjective,  $\forall n \in N \exists m \in M / u(m) = n$ , et par suite

$n^*(n) = k^*(n) \quad \forall n \in N$

d'où  $n^* = k^*$

cqfd

Remarque:  $M^*$  est toujours un  $A$ -module à droite si  $M$  est un  $A$ -module à gauche, grâce à la multiplication:  $M^* \times A \rightarrow M^*$

$m^*, a \mapsto m^* \cdot a / m^* \cdot a(x) =$

Plus  $t_u$  est  $A$ -linéaire.  $m^*(n) \cdot x a$  et il suffit de parler de Noëau.

Contre-exemples:

x)  $t_u$  injective ~~et~~  $u$  surjective

VOIR (\*) ci-dessous.

~~$M \xrightarrow{u} N$   
 $t_u$  injectif  $\Leftrightarrow \{t_u(\varphi) = 0 \Rightarrow \varphi = 0\} \Leftrightarrow \{\varphi \circ u = 0 \Rightarrow \varphi = 0\}$   
et  $u$  surjectif.~~

~~Prendre  $0 \xrightarrow{u} N \xrightarrow{\varphi} A$  où  $u$  non surjectif, et  $\varphi \circ u = 0$  et  $\varphi \neq 0$  cf (\*)  $\rightarrow$~~



B)  $u$  injective  $\nRightarrow \epsilon u$  surjective

$H \subset N \quad \epsilon u : H \rightarrow N$   
 $m \mapsto u(m) = m$  est injective.

Et pourtant,  $H = 2\mathbb{Z} \subset N = \mathbb{Z}$

$\psi : 2\mathbb{Z} \rightarrow \mathbb{Z}$

$2k \mapsto k$  est injective, et  $\psi \notin \text{Im}(\epsilon u)$ . En effet:

car si  $\psi(2) = 1$  et  $\psi(2) = 2\psi(1) \Rightarrow 1 = \text{paire ou nul}$   
 absurde.

donc  $\psi$  ne s'étend pas à  $\mathbb{Z}$ .

NB  $\psi \in \text{Im}(\epsilon u) \Leftrightarrow \exists n^* \in \mathbb{Z}^* / \psi(n^*) = n^*$

(\*) Exemple:  $\{0\} \xrightarrow{u} \mathbb{Z}/n\mathbb{Z} \quad n \geq 2$   
 injectif (comme  $\mathbb{Z}$ -modules)

On a bien  $\epsilon u : (\mathbb{Z}/n\mathbb{Z})^* \rightarrow \{0\}^*$   
 ~~$\epsilon u$  est injectif~~ car  $\text{Card}(\mathbb{Z}/n\mathbb{Z})^* > 1$   
 }  $u$  non surjectif.

$$\text{Card} \left\{ \underbrace{\text{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})}_{= \{0\}} \right\} = 1$$

Exercice:  $A$  anneau unitaire  
 $B$  ensemble

Trouver un  $A$ -module à gauche  $M$  tel que :

- 1) Il existe une injection  $B \xrightarrow{i} M$
- 2) Pour toute application  $B \xrightarrow{\varphi} N$  module à gauche, il existe un homomorphisme  $\bar{\varphi}: M \xrightarrow{\bar{\varphi}} N$  tel que  $\bar{\varphi} \circ i = \varphi$ , unique.

$$\begin{array}{ccc} & & \\ i \uparrow & \nearrow & \\ B & \xrightarrow{\varphi} & \end{array}$$

a) 2 solutions  $M_1$  et  $M_2$  sont isomorphes.

b) Il existe une solution  $M$ .

● Solution: a) On a

$$\begin{array}{ccc} M_1 & \xrightarrow{\beta} & M_2 \\ i_1 \uparrow & \nearrow i_2 & \\ B & & \end{array} \quad \beta \circ i_1 = i_2$$

De même, on a l'existence de  $g: M_2 \rightarrow M_1$  /  $g \circ i_2 = i_1$   
 donc  $g \circ \beta \circ i_1 = i_1$  où  $g \circ \beta: M_1 \rightarrow M_1$ .

$$\begin{array}{ccc} M_1 & \xrightarrow[g \circ \beta]{g \circ \beta} & M_1 \\ i_1 \uparrow & \nearrow i_1 & \\ B & & \end{array}$$

Le 2) montre l'unicité de  $\bar{\varphi}$ , donc ici :  $g \circ \beta = \text{Id}$ . De  $\hat{m}: \beta \circ g = \text{Id}$ , donc

●  $M_1$  et  $M_2$  sont isomorphes.

b)  $A^B = \{ (a_i)_{i \in B} \mid \text{applications } B \rightarrow A \}$  est un module à gauche sur  $A$ .

Posons  $A^{(B)} = \{ (a_i)_{i \in B} \mid \# \{ i \mid a_i \neq 0 \} < \infty \} \subset A^B$  est un sous-module à gauche de  $A^B$ .

(Note: Si  $B$  est fini  $A^B = A^{(B)}$ )

Montrons que  $A^{(B)}$  vérifie 1) et 2), et donc que  $A^{(B)}$  est solution :

• Pour le 1) : Soit  $i: B \rightarrow A^{(B)}$

$$b \mapsto i(b) = (a_{b'})_{b' \in B} \quad , \quad \begin{cases} a_{b'} = 0 \text{ si } b' \neq b \\ a_b = 1 \end{cases}$$

$i$  est injective.

Note :  $(a_b)_{b \in B} = \sum_{b \in B} a_b e_b$  où  $e_b = i(b) \in A^{(B)}$   
(somme finie)

Tous les éléments de  $A^{(B)}$  s'écrivent sous cette forme et de manière unique.  
On dit que  $(e_b)_{b \in B}$  est une base de l' $A$ -module  $A^{(B)}$ .

• Pour 3) : Soit  $\varphi: B \rightarrow N$   
 $b \mapsto \varphi(b)$

$$\begin{array}{ccc} A^{(B)} & \xrightarrow{\bar{\varphi}} & N \\ \uparrow i & \nearrow \varphi & \\ B & & \end{array}$$

Si  $\bar{\varphi}$  existe,

Nécessairement,  $\bar{\varphi} \circ i(b) = \varphi(b) \Leftrightarrow \bar{\varphi}(e_b) = \varphi(b)$

Donc, nécessairement,  $\bar{\varphi}\left(\sum_{b \in B} a_b e_b\right) = \sum_{b \in B} a_b \varphi(b)$

(Les sommes qui interviennent sont finies, et ont donc un sens dans les  $A$ -modules  $A^{(B)}$  et  $N$ )

Donc  $\bar{\varphi}$  est unique.

Montrons que  $\bar{\varphi}$  ainsi définie convient : on a

$$\begin{cases} (1) \bar{\varphi}(e_b) = \varphi(b) \\ (2) \bar{\varphi}((a_b)_{b \in B}) = \sum_{b \in B} a_b \varphi(b) \end{cases}$$

c.à.d que  $\bar{\varphi}$  est bien un homomorphisme de  $A$ -modules à gauche.

$$\begin{cases} \bar{\varphi}((a a_b)_{b \in B}) = \sum_{b \in B} a a_b \varphi(b) = a \bar{\varphi}((a_b)_{b \in B}) \\ \bar{\varphi}((a_b + c_b)_{b \in B}) = \bar{\varphi}((a_b)_{b \in B}) + \bar{\varphi}((c_b)_{b \in B}) \end{cases}$$

□ Q.F.D

Définition :  $A^{(B)}$  est le  $A$ -module libre à gauche construit sur  $B$ .

Remarque : \* On peut supprimer que l'hypothèse  $i$  injectif.

\* On n'a pas eu besoin de la propriété  $1.x = x$ .

## exercice 5

$M$  = module libre de type fini de base  $\{x_1, \dots, x_n\}$  sur  $A$  commutatif.

1)  $I$  idéal  $IM = \left\{ \sum_{i=1}^p a_i m_i \mid a_i \in I, m_i \in M \right\}$  = sous-module de  $M$ .

Montrer que  $M/IM$  est un  $A/I$ -module.

On sait (cf. cours) que  $M/IM$  sous-module de  $M$  =  $A$ -module.

Définissons  $\bar{k} \bar{m} = \overline{k m}$  où  $k \in A/I$  et  $\bar{m} \in M/IM$ . On le peut. En effet, si  $\bar{k} = \bar{k}' \Leftrightarrow k - k' \in I$

$$\bar{m} = \bar{m}' \Leftrightarrow m - m' = \sum_{i=1}^p a_i m_i \in IM$$

$$\text{Alors } k m - k' m' = k m + k' \left( \sum_{i=1}^p a_i m_i - m \right)$$

$$k m - k' m' = \underbrace{(k - k')}_{\in I} m + k' \sum_{i=1}^p a_i m_i \in IM$$

d'où :

Proposition :  $M$  module sur  $A$ , commutatif.  $I$  idéal de  $A$ .

$IM$  est un sous-module de  $M$

et  $M/IM$  est un  $A/I$ -module

$$\text{NB : } IM = \left\{ \sum_{i=1}^p a_i m_i \mid a_i \in I, m_i \in M \right\}$$

Proposition :

Supposons  $M$  libre. Alors  $M/IM$  est un module libre de type fini de base  $(\bar{x}_1, \dots, \bar{x}_n)$  sur  $A/I$

(R)  $m \in IM \quad \exists ! \lambda_k \in I \quad / \quad m = \sum_{k=1}^n \lambda_k x_k$ . En effet :

$$\left\{ \begin{array}{l} \forall m \in IM \\ \exists a_i \in I \end{array} \right. \quad m = \sum_{i=1}^p a_i m_i = \sum_{i=1}^p a_i \sum_{j=1}^n b_{ij}^i x_j = \sum_{j=1}^n \left( \sum_{i=1}^p a_i b_{ij}^i \right) x_j$$

$\underbrace{\sum_{i=1}^p a_i b_{ij}^i}_{\in I}$

Moynant cette remarque (R), la démonstration de la proposition est facile :

$$\forall \tilde{x} \in M/IM \quad \exists \lambda_i \in A \quad / \quad x = \sum_{i=1}^n \lambda_i x_i$$

$$\text{d'où } \tilde{x} = \sum_{i=1}^n \lambda_i \tilde{x}_i$$

ce qui prouve que  $(\tilde{x}_1, \dots, \tilde{x}_n)$  est un système générateur dans  $M/IM$ .

De plus,  $M/IM$  c'est une base ! En effet, considérons la combinaison linéaire  $\sum_{i=1}^n \lambda_i \tilde{x}_i = 0 \Rightarrow \sum_{i=1}^n \lambda_i x_i \in IM \Rightarrow \lambda_i \in I \quad \forall i \Rightarrow \lambda_i = 0 \quad \forall i$  (cf R)

Ce qui prouve que  $M/IM$  est libre de type fini.

a)

$\mathbb{R}$

$\mathfrak{m}$  idéal maximal donc  $A/\mathfrak{m}$  est un corps.

~~$M/IM$~~   $M/\mathfrak{m}M$  est un  $A/\mathfrak{m}$ -module.  $\Rightarrow$   $M/\mathfrak{m}M$  est un  $A/\mathfrak{m}$ -espace vectoriel

Remarque: Dans ce cas où  $M$  est un module libre de type fini, on remarque que pour tout  $\mathfrak{m}$  idéal maximal,  $M/\mathfrak{m}M$  est un corps de dimension  $n$ , constante.

maidi 5 février 80

②  $M = A$ -module  $A$  anneau commutatif.

1°/ déterminer  $\text{Hom}_A(A, M)$

Si  $\varphi \in \text{Hom}_A(A, M)$ , on a  $\forall a \in A \quad \varphi(a \cdot 1) = a \varphi(1)$

d'où  $\varphi: \text{Hom}_A(A, M) \rightarrow M$

$\varphi \mapsto \varphi(1)$

$\varphi$  est bijective.

(d'ailleurs, si  $x \in M$  est fixé,  $\varphi(a) = ax$  est antécédent de  $x$ ).

Tout cela est très simple.

2°/  $M^* = \text{Hom}_A(M, A)$  est un  $A$ -module pour les opérations suivantes

$\forall \begin{cases} \beta, \gamma \in M^* \\ \alpha \in A \end{cases}$  on a  $(\beta + \gamma) \in M^*$  et  $\alpha\beta \in M^*$  car :

$$\begin{cases} (\alpha\beta)(x+y) = \alpha\beta(x+y) = \alpha\beta(x) + \alpha\beta(y) \\ (\alpha\beta)(bx) = \alpha b\beta(x) = b\alpha\beta(x) \text{ car } A \text{ comm} \end{cases}$$

# Définition de $H \rightarrow H^{**}$

$$h: H \rightarrow H^{**}$$

$$\alpha \mapsto \hat{\alpha}(\beta) = \beta(\alpha)$$

$h$  est un homomorphisme de  $A$ -modules.

Calculons, par exemple  $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) = \{0\}$

En effet,  $\varphi \in \text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) \Rightarrow \varphi(\underbrace{n \cdot 1}_{\varphi(0)}) = n\varphi(1) \Rightarrow \varphi(1) = 0$

Donc:

$h$  n'est pas injective, où  $h: \mathbb{Z}/n\mathbb{Z} \rightarrow \{0\}$ .

Si  $p|q$ , il est clair que  $\mathbb{Z}/p\mathbb{Z}$  est un  $\mathbb{Z}/q\mathbb{Z}$ -module.

Si  $p \nmid q$ , considérons  $\text{Hom}_{\mathbb{Z}/q\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/q\mathbb{Z}) = (\mathbb{Z}/p\mathbb{Z})^*$ . (P)

Remarque: Si  $A \xrightarrow{\varphi} B$  est un homomorphisme d'anneaux, et si  $M$  est un  $B$ -module, alors la multiplication  $M \times A \rightarrow M$  est un  $A$ -module, d'une façon canonique.

$$(m, a) \mapsto \varphi(a)m$$

En utilisant cette remarque, on voit bien que  $\mathbb{Z}/p\mathbb{Z}$  est un  $\mathbb{Z}/q\mathbb{Z}$ -module ( $p|q$ ) pour la multiplication externe

$$\begin{array}{ccc} \pi \cdot y & = & \pi y \\ \uparrow & & \uparrow \\ \text{mod } q & & p \end{array} \quad (\text{bien définie})$$

## Solution de (P)

Soit  $q = pn$

Notons  $(\mathbb{Z}/p\mathbb{Z})^* = \text{Hom}_{\mathbb{Z}/q\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/q\mathbb{Z})$ .

et considérons  $\varphi \in (\mathbb{Z}/p\mathbb{Z})^*$ .

On a:  $\varphi(\overline{y}^p) = \varphi(\overline{1}^q \cdot \overline{y}^p) = \varphi(\overline{1}^q \cdot \overline{y} \cdot \overline{1}^p) = \varphi(\overline{y}^q \cdot \overline{1}^p) = \overline{y}^q \varphi(\overline{1}^p)$

Donc, si  $\varphi: (\mathbb{Z}/p\mathbb{Z})^* \rightarrow \mathbb{Z}/q\mathbb{Z}$  est définie  
 $\varphi \mapsto \varphi(\overline{1}^p)$  est injective  
 et est un homomorphisme de  $(\mathbb{Z}/q\mathbb{Z})$ -module.

Cherchons  $\text{Im } \varphi$ .

Soit  $\bar{a}^q \in \mathbb{Z}/q\mathbb{Z}$ . Cherchons  $\varphi / \varphi(\bar{1}^p) = \bar{a}^q$

~~Grâce à~~  $\exists \varphi / \varphi(\bar{1}^p) = \bar{a}^q \Leftrightarrow \exists \varphi / \varphi(\bar{k}^p) = k \bar{a}^q \quad \forall k \in \mathbb{Z}$

$$\Leftrightarrow \exists \varphi / \varphi(\bar{0}) = p \bar{a}^q$$

$$\Leftrightarrow q / p a \Leftrightarrow n | a$$

Ainsi  $\mathcal{g}((\mathbb{Z}/p\mathbb{Z})^{\times}) = \{ \bar{a}^q \in \mathbb{Z}/q\mathbb{Z} / n | a \}$

$$= n(\mathbb{Z}/q\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}$$

Ainsi

$$\text{Hom}_{\mathbb{Z}/q\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/q\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}$$

⑥ 1)  $\text{Hom}_A(A^n, A) \simeq A^n$  (Suite du TD: feuille 5 de la même série.)

2)  $u: M \rightarrow N$   $A$ -linéaire

$$M^* \xrightarrow{u^*} N^* / u^*(n^*) = n^* \circ u$$

I.M.S.P.

MATHEMATIQUES

M 1 ALGEBRE - PARTIEL DU 31 MARS 1978

Durée : 3 HEURES

---

Les exercices 1, 2, 3, 4 sont indépendants. Leur solution exige plus de réflexion que de connaissances ...

I . Soit  $f : \mathbb{Z}^2 \rightarrow \mathbb{Z}^2$  un homomorphisme, de matrice  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  .

Donner une CNS sur les entiers  $a, b, c, d$  pour que le groupe  $\mathbb{Z}^2 / \text{Im } f$  soit cyclique. Préciser la structure du groupe  $\mathbb{Z}^2 / \text{Im } f$  dans le cas de la matrice  $\begin{pmatrix} 2 & 4 \\ -6 & 0 \end{pmatrix}$  .

II . Soit  $K$  un corps fini. On choisit au hasard un élément  $c$  parmi les éléments de  $K$  , supposés équiprobables. Quelle est la probabilité pour que le polynôme  $x^2 + x - c = 0$  soit irréductible sur  $K$  ? on distinguera les cas  $\text{car}_2 K = 2$  ,  $\text{car}_2 K \neq 2$  .

III . Soit  $P$  un polynôme de degré  $n$  à coefficients entiers. On pose

$$Q(X) = P(X + P(X))$$

a/ Quel est le degré de  $Q$  ? Il y a un cas particulier !

b/ Montrer que  $P(X)$  divise  $Q(X)$

c/ En déduire qu'il n'existe pas de polynôme  $P \in \mathbb{Z}[X]$  , non constant, tel que :

$$\forall n \in \mathbb{Z} , \quad P(n) \text{ est premier.}$$

IV . Soit  $G_p = (\mathbb{Z} / p\mathbb{Z})^*$  le groupe multiplicatif du corps  $\mathbb{Z} / p\mathbb{Z}$  .  
On suppose  $p \neq 2$  . On rappelle que  $G_p$  est cyclique



a/ Soit  $a$  un générateur de  $G_p$ . Montrer que

$$(a)^{\frac{p-1}{2}} = -1$$

b/ Montrer que  $x \in G_p$  est le carré d'un élément  $y \in G_p$  si et seulement si :

$$(x)^{\frac{p-1}{2}} = 1.$$

c/ On considère l'entier

$$k = \frac{p-1}{2}$$

$$A = \prod_{k=1}^k (2k) = 2 \cdot 4 \cdot \dots \cdot (p-3)(p-1)$$

En distinguant les cas  $\left(\frac{p-1}{2}\right)$  pair,  $\frac{p-1}{2}$  impair, montrer que

$$A \equiv (-1)^{u(p)} \left(\frac{p-1}{2}\right)! \pmod{p}$$

où  $u(p)$  est une fonction de  $p$  que l'on précisera dans chaque cas.

En déduire que  $2^{\frac{p-1}{2}} \equiv (-1)^{u(p)}$  et indiquer pour quelles valeurs de  $p$  la classe de 2 est un carré dans  $\mathbb{Z} / p\mathbb{Z}$

d/ Montrer que  $X^3 + X^2 - 3X + 1$  a trois racines dans  $\mathbb{Z} / 97\mathbb{Z}$  (il n'est pas interdit de les chercher).

Partiel du 31 mars 1978

①  $f: \mathbb{Z}^2 \rightarrow \mathbb{Z}^2$  de matrice  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$\exists$  base  $(e_1, e_2)$  de  $\mathbb{Z}^2$ -départ

$\exists$  base  $(f_1, f_2)$  de  $\mathbb{Z}^2$ -arrivée telles que

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \sim \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}$$

matrice dans les nouvelles bases.

où  $d_1 = \Delta(a, b, c, d)$  et  $d_1 \mid d_2$ .

$d_2 = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$

Alors  $\text{Im } f \cong d_1 \mathbb{Z} \times d_2 \mathbb{Z}$

$$\mathbb{Z}^2 / \text{Im } f \cong \mathbb{Z}^2 / d_1 \mathbb{Z} \times d_2 \mathbb{Z} \cong \mathbb{Z} / d_1 \mathbb{Z} \times \mathbb{Z} / d_2 \mathbb{Z}$$

NB:  $\mathbb{Z}$  cyclique  $\Leftrightarrow$  monogène (pas forcément fini)

• Si  $d_1 = d_2 = 0$   $f = 0 \Rightarrow \text{Im } f = \{0\}$  d'où  $\mathbb{Z}^2 / \text{Im } f \cong \mathbb{Z}^2_{\text{non cyclique}}$ .

• Si  $d_2 = 0$   $\mathbb{Z}^2 / \text{Im } f \cong \mathbb{Z} / d_1 \mathbb{Z} \times \mathbb{Z}$  ( $d_1 \neq 0$ )

S'il était cyclique, il existerait un isomorphisme de groupe de  $\mathbb{Z}^2 / \text{Im } f$  sur  $\mathbb{Z}_n \mathbb{Z}$  ou sur  $\mathbb{Z}$ . Si  $\varphi: \mathbb{Z}^2 / \text{Im } f \rightarrow \mathbb{Z}_n \mathbb{Z}$ , on aurait un élément [à savoir  $(0, 1) \in \mathbb{Z} / d_1 \mathbb{Z} \times \mathbb{Z}$ ] d'ordre infini. Donc  $\varphi: \mathbb{Z}^2 / \text{Im } f \rightarrow \mathbb{Z}$ .

Mais, de la même façon, il y aurait un élément d'ordre fini. Donc  $\mathbb{Z}^2 / \text{Im } f$  non cyclique.

• Si  $d_1$  et  $d_2$  non nuls,  $\mathbb{Z}^2 / \text{Im } f \cong \mathbb{Z} / d_1 \mathbb{Z} \times \mathbb{Z} / d_2 \mathbb{Z}$

$\Delta(d_1, d_2) = 1 \Leftrightarrow \mathbb{Z}^2 / \text{Im } f \cong \mathbb{Z} / d_1 d_2 \mathbb{Z}$  (Th. Chinois)

Ainsi :  $\mathbb{Z}^2 / \text{Im } f$  cyclique  $\Leftrightarrow \text{GCD}(d_1, d_2) = 1 \Leftrightarrow \underline{d_1 = 1}$  (car  $d_1 | d_2$ )

Cas de  $M = \begin{pmatrix} 2 & 4 \\ -6 & 0 \end{pmatrix}$

$$\S \quad \begin{pmatrix} 2 & 4 \\ -6 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 12 \\ -6 & 0 \end{pmatrix} \begin{pmatrix} 2 & 4 \\ 0 & 12 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 \\ 0 & 12 \end{pmatrix}$$

$$\mathbb{Z}^2 / \text{Im } f \simeq \mathbb{Z} / 2\mathbb{Z} \times \mathbb{Z} / 12\mathbb{Z} \quad \text{non cycliques.}$$

③  $K = \text{corps fini}$ .

$$c \in K \quad x^2 + x - c = 0 \text{ irréductible sur } K$$

$$\textcircled{3} \quad P \in \mathbb{Z}[X] \quad Q(X) = P(X + P(X))$$

a) \* Si  $\deg P \geq 2$        $\deg Q(X) = (\deg P)^2$

\* Si  $\deg P = 1$  :

$$\begin{cases} \deg Q = 1 & \text{si } P = -X + cte \\ \deg Q = 0 & \text{si } P = -X + cte \end{cases}$$

\* Si  $\deg P = 0$ ,       $\deg Q = 0$ .

Ainsi :

$$\deg Q = (\deg P)^2 \text{ sauf si } P = -X + cte, \text{ auquel cas } \deg Q = 0$$

b)  $P(X)$  divise  $Q(X)$

1<sup>re</sup> méthode

$$P \in \mathbb{Z}[X] \subset \mathbb{Q}[X]$$

Soit  $\alpha \in \mathbb{Q} / P(\alpha) = 0$ . Alors  $Q(\alpha) = P(\alpha + P(\alpha)) = 0$

Toute racine de  $P$  est racine de  $Q$ . Cela n'est pas suffisant pour affirmer que  $P \mid Q$ . Montrons que :

$$\alpha \text{ racine de } P \text{ de multiplicité } k \Rightarrow \alpha \text{ rac. de } Q \text{ de mult. } k \text{ au moins. (R)}$$

Alors, si (R) est prouvé, on aura :  $P \mid Q$ , puisque :

$$\left\{ \begin{array}{l} P = (X - \alpha_1)^{k_1} \dots (X - \alpha_m)^{k_m} \\ \text{et} \\ Q = (X - \alpha_1)^{l_1} \dots (X - \alpha_m)^{l_m} Q_1(X) \end{array} \right.$$

Preuve de (R)

Récurrence finie sur l'ordre de  $\alpha$ .

Soit  $\alpha$  d'ordre  $k > 1$  de  $P(X)$ ;  $P(n) = "(X - \alpha)^n \text{ divise } Q(X)"$ .

•  $P(1)$  vrai.

Montrons que  $\forall n \in [1, k-1]$   $P(n) \Rightarrow P(n+1)$  vraie.

Soit  $P(n)$  vraie :  $(X-\alpha)^n \mid Q(X)$ .

$$\text{Ainsi } \begin{cases} Q(X) = (X-\alpha)^n Q_1(X) \\ \text{or } P(X) = (X-\alpha)^n P_1(X) \end{cases}$$

$$\begin{aligned} \text{d'où } Q(X) = P(X+P(X)) &\Rightarrow (X-\alpha)^n Q_1(X) = (X+P(X)-\alpha)^n P_1(X+P(X)) \\ &\Rightarrow (X-\alpha)^n Q_1(X) = [(X-\alpha)(1+(X-\alpha)^{-1}P_1(X))]^n P_1(X+P(X)) \end{aligned}$$

$$\begin{aligned} \text{d'où } (X-\alpha)^n Q_1(X) &= (X-\alpha)^n (1+(X-\alpha)^{-1}P_1(X))^n P_1(X+P(X)) \\ Q_1(X) &= (1+(X-\alpha)^{-1}P_1(X))^n P_1(X+P(X)) \end{aligned}$$

$$\text{donc } Q_1(\alpha) = P_1(\alpha + P(\alpha)) = P_1(\alpha) = 0 \quad \text{car } P_1(\alpha) = 0.$$

$$\text{d'où } Q(X) = (X-\alpha)^{n+1} Q_2(X) \Rightarrow P(n+1) \text{ vraie.}$$

Conclusion :  $P(k)$  vraie, c.à.d.  $(X-\alpha)^k \mid Q(X)$ .

2<sup>e</sup> méthode

$$\begin{cases} P(X) = \sum_{k=0}^n a_k X^k \\ Q(X) = \sum_{k=0}^n a_k (X^k + P(X) \cdot R_k(X)) \end{cases} \quad \text{et tac! ?}$$

$$c) \quad \underline{P \in \mathbb{Z}[X] / \forall n \in \mathbb{Z} \quad P(n) \text{ premier} \Rightarrow P = cte \in \mathbb{Z}}$$

Si  $P$  convient, alors  $P(n) \mid Q(n)$  et  $Q(n) = P(n + P(n))$  premier.

$$\text{Donc } P(n) = Q(n) \quad \forall n \in \mathbb{N} \quad (\text{car } P(n) \neq 1)$$

$R(X) = P(X) - Q(X)$  possède alors une infinité de racine. Tout polynôme de  $\mathbb{Z}[X]$  de degré  $n$  admet au plus  $n$  racines (car  $\mathbb{Z}$  anneau com. et intègre). Donc  $P(X) = Q(X) \Rightarrow \begin{cases} (\deg P)^2 = \deg P \\ \text{ou} \\ 0 = \deg P \end{cases}$  et  $P \neq -X + cte$  ou  $P = -X + cte$ , imp.

$$P(X) = Q(X) \Rightarrow [\deg P = 1 \text{ ou } \deg P = 0 \text{ et } P \neq -X + cte]$$

$$\Rightarrow \begin{cases} \deg P = 0 & (1) \\ \text{ou} \\ \deg P = 1 \text{ et } P \neq -X + cte & (2) \end{cases}$$

Montrons que le (2) ne peut pas se produire. Supposons que  $P(X) = aX + b$  où  $a \neq 0$  et  $a \neq -1$ .

$$P(X + P(X)) = a(a+1)X + ab + b = P(X) = aX + b$$

$$\Downarrow$$

$$a = a(a+1)$$

$$\Downarrow$$

$$1 = a + 1$$

$$\Downarrow$$

$$a = 0 \text{ non}$$

Donc

$$P \in \mathbb{Z}[X] / \forall n \in \mathbb{Z} \quad P(n) \text{ premier} \Rightarrow P = cte \in \mathbb{Z}$$

cqfd

④  $G_p = \mathcal{U}(\mathbb{Z}/p\mathbb{Z})$  où  $p$  premier.  $p \neq 2$ .

a)  $a$  g  n  rateur de  $G_p \Leftrightarrow \begin{cases} a^{p-1} = 1 \\ a^k \neq 1 \quad \forall k \in [1, p-2] \end{cases}$

Puisque  $p = 2p' + 1$ .

Donc  $a^{p-1} = 1 \Leftrightarrow (a^{p'})^2 = 1 \Rightarrow a^{p'} = \pm 1$

Comme  $a^{p'} \neq 1$ ,  $a^{p'} = -1$ .

b)  $x \in G_p \text{ } \{ x = y^2 \Leftrightarrow x^{p'} = 1 \}$

Si  $x = y^2$  alors  $x^{p'} = y^{2p'} = y^{p-1} = 1$  oui.

Inversement, si  $x^{p'} = 1$ ,  $x = a^k$  o    $a$  g  n  rateur de  $G_p$ .

$a^{kp'} = 1 \Rightarrow (a^{p'})^k = 1 \Rightarrow (-1)^k = 1 \Rightarrow k \equiv 0 [2]$

d'o    $k = 2k'$   $x = (a^2)^{k'}$

$k = p'$

c)  $A = \prod_{k=1}^{p-1} (2k) = 2 \cdot 4 \cdot \dots \cdot (p-3) \cdot (p-1)$

$p' = \frac{p-1}{2}$

$A \equiv (-1)^{u(p)} \frac{(p-1)!}{(p')!} [p]$

Si  $\frac{p-1}{2}$  pair

$\equiv 1 - p' [p]$

$A = 2 \times 4 \times 6 \dots \times p' \times (p'+2) \times \dots \times (p-1) \equiv 2 \times 4 \times \dots \times p' \times (2+p'-p) \times \dots \times (-1) \equiv (-1)^{p'} [p]$

$$A = \cancel{2 \times 4 \times \dots \times p'} \times \underbrace{(-1)(p'+2)p'}_{\frac{p'}{2} \text{ terms}} \times \dots \times (-1)$$

$$A = (-1)^{\frac{p'}{2}} (p')!$$

$$\boxed{\frac{p-1}{2} \text{ impair}} \quad p = 2p' + 1$$

$$\equiv -p' [p]$$

$$A = \underbrace{2 \times 4 \times 6 \times \dots \times (p'-1)}_{\frac{p'-1}{2} \text{ terms}} \times \underbrace{(p'+1)(p'+2)}_{\equiv 3-p' [p]} \times \dots \times \underbrace{(p-1)}_{\equiv -1 [p]}$$

$$A = (-1)^{\frac{p'-1}{2}} (p')!$$

$$\left\{ \begin{array}{l} \text{Si } \frac{p-1}{2} \text{ pair } u(p) = (-1)^{\frac{p-1}{4}} \\ \text{Si } \frac{p-1}{2} \text{ impair } u(p) = (-1)^{\frac{p-3}{4}} \end{array} \right.$$

$$A = 2^{\frac{p-1}{2}} \prod_{k=1}^{\frac{p-1}{2}} k \Rightarrow 2^{\frac{p-1}{2}} \prod_{k=1}^{\frac{p-1}{2}} k \equiv \left(\frac{p-1}{2}\right)! (-1)^{u(p)} [p]$$

$\Downarrow$

$$2^{\frac{p-1}{2}} \equiv (-1)^{u(p)} [p]$$

( $2/p \not\equiv$  intègre)



$$2 \text{ est un carré dans } \mathbb{Z}/p\mathbb{Z} \Leftrightarrow 2^{\frac{p-1}{2}} \equiv 1 \Leftrightarrow (-1)^{u(p)} \equiv 1 \quad [p]$$

$$\Leftrightarrow u(p) \text{ pair} \quad (1)$$

$$\left\{ \begin{array}{l} \text{Si } \frac{p-1}{2} \text{ pair, } (1) \Leftrightarrow \frac{p-1}{4} \equiv 0 \quad [2] \Leftrightarrow p-1 = 8k \Leftrightarrow p \equiv 1 \quad [8] \quad (2) \\ \text{Si } \frac{p-1}{2} \text{ impair, } (1) \Leftrightarrow \frac{p-3}{4} \equiv 0 \quad [2] \Leftrightarrow p-3 = 8k \Leftrightarrow p \equiv 3 \quad [8] \quad (3) \end{array} \right.$$

$$\left\{ \begin{array}{l} (3): \text{ Si } p = 3 + 8k \quad \frac{p-1}{2} = \frac{2+8k}{2} = 1+4k \quad \text{pas de contradiction} \\ (2) \end{array} \right.$$

$$d) \quad X^3 + X^2 - 3X + 1 = 0$$

$$\mathbb{Z}/97\mathbb{Z}$$

$$(X-1)(X^2 + \alpha X - 1) \quad \text{où } \alpha = \cancel{2}$$

$$(X-1)(X^2 + 2X - 1) = 0$$

$$(X-1)(X-1)^2 = 0$$

$$\left\{ \begin{array}{l} X=1 \\ \text{ou} \\ X^2 + 2X - 1 = 0 \end{array} \right.$$

$$X^2 + 2X - 1 = (X+1)^2 - 2 = 0$$

$$(X+1)^2 = 2$$

$$\exists 2 \text{ sol à cette équationssi } 2 \text{ est un carré dans } \mathbb{Z}/97\mathbb{Z} \quad \frac{97-1}{2} = 48 \text{ pair}$$

## Exercice

Montrer que  $\dim(E_1 + E_2) = \dim E_1 + \dim E_2 - \dim(E_1 \cap E_2)$  (1)

1° 1<sup>re</sup> méthode

Introduire  $I = E_1 \cap E_2$  et  $\begin{cases} F_1 \oplus I = E_1 \\ F_2 \oplus I = E_2 \end{cases}$  etc...

2° 2<sup>e</sup> méthode

a) On considère  $f: E_1 \times E_2 \rightarrow E$   
 $(x_1, x_2) \mapsto x_1 + x_2$

Montrer que  $f$  est linéaire

b) Montrer que  $\ker f = \{(x, -x) \mid x \in E_1 \cap E_2\}$

En déduire que  $\ker f$  est isomorphe à  $E_1 \cap E_2$

c) Démontrer que  $\operatorname{Im} f = E_1 + E_2$

En déduire que l'on a la formule (1)

Sol

1°

Posons  $I = E_1 \cap E_2$

$I \oplus F_1 = E_1$

$I \oplus F_2 = E_2$

d'où:

$$\dim I + \dim F_1 = \dim E_1$$

$$\dim I + \dim F_2 = \dim E_2$$

$$\dim F_1 + \dim F_2 + \dim(E_1 \cap E_2) = \dim E_1 + \dim E_2 - \dim(E_1 \cap E_2)$$

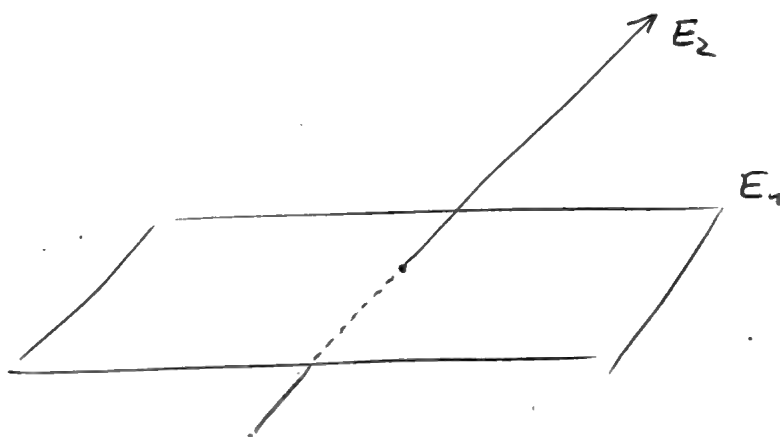
Montrons que  $F_1 \oplus F_2 \oplus (E_1 \cap E_2) = E_1 + E_2$

$$\text{Soit } x = \underbrace{x_1}_{\in E_1} + \underbrace{x_2}_{\in E_2}, \text{ alors } x = \underbrace{x_1^I}_{\in I} + \underbrace{x_1^{F_1}}_{\in F_1} + \underbrace{x_2^I}_{\in I} + \underbrace{x_2^{F_2}}_{\in F_2}$$

$$x = \underbrace{x_1^I + x_2^I}_{\in I} + \underbrace{x_1^{F_1} + x_2^{F_2}}_{\in F_1 + F_2}$$

$$\text{donc } E_1 + E_2 \subset F_1 + F_2 + E_1 \cap E_2$$

de plus, cette somme est directe car :



$$\begin{cases} F_1 \cap F_2 \cap (E_1 \cap E_2) = \{0\} \\ \text{et} \\ F_1 \cap F_2 = \{0\} \end{cases}$$

$$\text{d'où } E_1 + E_2 \subset F_1 \oplus F_2 \oplus E_1 \cap E_2$$

$$\text{Inversement, soit } x = \underbrace{x_1}_{\in F_1} + \underbrace{x_2}_{\in F_2} + \underbrace{x_I}_{\in E_1 \cap E_2} \in F_1 \oplus F_2 \oplus E_1 \cap E_2$$

$$\text{Alors } x = \underbrace{x_1 + \frac{x_I}{2}}_{\in E_1} + \underbrace{x_2 + \frac{x_I}{2}}_{\in E_2} \Rightarrow x \in E_1 + E_2$$

2°/

a) évident

$$\begin{aligned} \text{b) } \text{Ker } f &= \{ (x_1, x_2) \in E_1 \times E_2 \mid x_1 = -x_2 \} \\ &= \{ (x, -x) \mid x \in E_1 \cap E_2 \} \end{aligned}$$

On exhibe l'isomorphisme d'e.v.:

$$\begin{aligned} \varphi : E_1 \cap E_2 &\longrightarrow \text{Ker } f \\ x &\longmapsto (x, -x) \end{aligned}$$

$$\text{c) } \text{Im } f = E_1 + E_2 \quad (\text{évident})$$

Conclusion :  $\dim \text{Ker } f + \dim \text{Im } f = \dim E_1 \times E_2$

$$\dim(E_1 \cap E_2) + \dim(E_1 + E_2) = \dim E_1 + \dim E_2$$

$$\boxed{\dim(E_1 + E_2) = \dim E_1 + \dim E_2 - \dim(E_1 \cap E_2)}$$

① 163 p 296

$$E_0, E_1, \dots, E_n = \text{e.v. sm } K \quad (n \geq 1)$$

Pf:

$$E_0 \xrightarrow{f_0} E_1 \rightarrow \dots \rightarrow E_{k-1} \xrightarrow{f_{k-1}} E_k \xrightarrow{f_k} E_{k+1} \rightarrow \dots \xrightarrow{f_{n-1}} E_n$$

est une suite exacte si

$$\text{Im } f_k = \text{Ker } f_{k+1} \quad \forall k \in [0, n-2]$$

$$a) [0 \rightarrow E \xrightarrow{f} F \text{ est une suite exacte}] \Leftrightarrow f \text{ injective}$$

$\exists !$  l linéaire de 0 vers E, à savoir:  $l(0) = \vec{0}_E$

$$\bullet (\Leftarrow) f \text{ injective} \Rightarrow \text{Ker } f = \{\vec{0}_E\} \Rightarrow \text{Im } l = \text{Ker } f.$$

$$(\Rightarrow) \underbrace{\text{Im } l}_{\substack{= \\ \{\vec{0}_E\}}} = \text{Ker } f \Rightarrow f \text{ injective.}$$

$$[E \xrightarrow{f} F \xrightarrow{l} 0 \text{ est une suite exacte}] \Leftrightarrow f \text{ surjective}$$

$$\text{En effet: } f \text{ surjective} \Leftrightarrow f(E) = F = \text{Ker } l \Leftrightarrow [E \xrightarrow{f} F \xrightarrow{l} 0 \text{ exacte}]$$

b)

$$0 \xrightarrow{l} F \xrightarrow{i} E \xrightarrow{s} E/F \xrightarrow{l'} 0$$

$$\left\{ \begin{array}{l} \text{Ker } i = \{\vec{0}\} \quad (\text{car } i \text{ inj.}) \\ \text{Ker } s = F = \text{Im } i \\ \text{Ker } l' = \text{Im } s \quad (\text{car } s \text{ surj.}) \end{array} \right.$$

$$0 \xrightarrow{l} \text{Ker } f \xrightarrow{i} E \xrightarrow{f} F \xrightarrow{s} F/\text{Im } f \xrightarrow{l'} 0$$

$$\left\{ \begin{array}{l} \text{Ker } i = \{\vec{0}\} \text{ car } i \text{ injective} \\ \text{Ker } l' = F/\text{Im } f \text{ car } s \text{ surj.} \end{array} \right.$$

De plus :

$$* \text{Ker } \beta = \text{Im } i$$

$$\begin{aligned} * \text{Ker } \alpha &= \{ x \in F / \alpha(x) = 0 \in F / \text{Im } \beta \} \\ &= \{ x \in F / x \in \text{Im } \beta \} \\ &= \text{Im } \beta \end{aligned}$$

CQFD

169 p 297

a)

$$0 \rightarrow E_0 \xrightarrow{\beta_0} \dots \rightarrow E_k \xrightarrow{\beta_k} E_{k+1} \rightarrow \dots \xrightarrow{\beta_{n-1}} E_n \rightarrow 0$$

Bilan

$$\boxed{\sum_{2k+1 \leq n} \dim E_{2k+1} = \sum_{2k \leq n} \dim E_{2k}} \quad (1)$$

$$\forall k \in \{0, n-1\} \quad \dim \text{Im } \beta_k + \frac{\dim \text{Ker } \beta_k}{\dim \text{Im } \beta_{k-1}} = \dim E_k$$

$$\dim \text{Im } \beta_0 = \dim E_0$$

$$\dim \text{Im } \beta_1 + \dim \text{Im } \beta_0 = \dim E_1$$

$$\dim \text{Im } \beta_2 + \dim \text{Im } \beta_1 = \dim E_2$$

---

$$\dim \text{Im } \beta_{n-1} + \dim \text{Im } \beta_{n-2} = \dim E_{n-1}$$

$$\dim \text{Im } \beta_{n-1} = \dim E_n$$

$$\boxed{\dim E_0 - \dim E_1 + \dots + (-1)^n \dim E_n = 0} \quad (2)$$

3

On n'a toujours pas montré (1)

En ajoutant seulement les lignes paires du système (I),

nous obtenons: \* Si n pair

$$\dim E_0 + \dim E_2 + \dots + \dim E_n = \sum_{k=1}^{n-1} \dim \operatorname{Im} f_k$$

et:

$$\dim E_1 + \dim E_3 + \dots + \dim E_{n-1} = \sum_{k=1}^{n-1} \dim \operatorname{Im} f_k$$

• d'où l'égalité (1)

\* Si n impair: m dem.

Remarque: on peut ne pas considérer de cas n pair ou impair, et se rappeler de de Bcs:

$$2E\left(\frac{n-1}{2}\right) = \begin{cases} n \text{ impair} \rightarrow n-1 \\ n \text{ pair} \rightarrow n \end{cases}$$

• 1)  $0 \rightarrow E \cap F \xrightarrow{\beta+\gamma} E \oplus F \xrightarrow{\alpha-\gamma} E+F \rightarrow 0$

\*  $\mathcal{E}$  est une suite exacte

\* on en déduit la formule  $\dim(E+F) + \dim(E \cap F) = \dim E \oplus F$

M. 1: ALGÈBRE - DURÉE / 3H

mercredi 14 Juin

I

Soit  $G$  un groupe,  $H$  et  $K$  deux sous-groupes de  $G$ . Montrer que  $G = H \cup K$  entraîne  $G = H$  ou  $G = K$  (utiliser une partition de  $G$  en classes à gauche).

II

On considère l'application

$$f : \mathbb{Z}^3 \longrightarrow \mathbb{Z}^2$$

$$(x, y, z) \longmapsto (2x - 3y, x + 6y - 3z)$$

- 1) Montrer que  $\mathbb{Z}^2 / \text{Im } f$  est un groupe cyclique dont on déterminera l'ordre  $n$ .
- 2) Définir un homomorphisme surjectif  $g : \mathbb{Z}^2 \rightarrow \mathbb{Z} / n\mathbb{Z}$  de noyau  $\text{Im } f$ .
- 3) Déterminer le noyau de  $f$ .
- 4) Résoudre le système

$$2x - 3y = 5$$

$$x + 6y - 3z = 1$$

III

Soit  $E$  l'ensemble des polynômes de degré  $\leq n$ , à coefficients rationnels, tels que

$$\forall P \in E, \forall m \in \mathbb{Z}, P(m) \in \mathbb{Z}$$

Il est clair que  $E$  est un sous-groupe de  $(\mathbb{Q}[X], +)$

a) En considérant l'application

$$F : E \longrightarrow \mathbb{Z}^{n+1}$$

$$P \longmapsto (P(0), P(1), \dots, P(n))$$

montrer que  $E$  est un groupe abélien libre de rang  $\leq n + 1$ .

- b) Construire un homomorphisme injectif de  $\mathbb{Z}^{n+1}$  dans  $E$ . Conclure.  
(On considèrera les polynômes à coefficients entiers).
- c) On considère les polynômes

$$P_0(X) = 1, \quad P_1(X) = X, \quad \dots, \quad P_k(X) = \frac{X(X-1) \dots (X-k+1)}{k!} \dots$$

pour  $0 \leq k \leq n$ .

Soit  $E'$  le sous-groupe de  $E$  engendré par ces polynômes. Montrer (en étudiant sa matrice) que la restriction de  $F$  à  $E'$  est une bijection de  $E'$  sur  $\mathbb{Z}^{n+1}$ . Que peut-on en conclure ?



Énoncés

- ① Déterminer les nombres  $n$  pour lesquels  $U(\mathbb{Z}/n\mathbb{Z})$  est isomorphe à  $(\mathbb{Z}/2\mathbb{Z})^k$ .
- ② Soit  $A$  une  $\mathbb{R}$ -algèbre commutative, de dimension 2.  $\alpha)$  Montrer que  $A$  est isomorphe à un quotient  $\mathbb{R}[X]/(P)$  où  $\deg P = 2$ . (on note  $(P) = P\mathbb{R}[X]$ )  
 $\beta)$  En discutant sur  $P$ , montrer que  $A$  est isomorphe à l'une des 3 algèbres suivantes :
- \*  $\mathbb{C}$
  - \*  $\mathbb{R}[X]/(X^2)$  ou  $\mathbb{R} \oplus \mathbb{R} \varepsilon$  (nbres duaux, ou développements limités à l'ordre 2)
  - \*  $\mathbb{R}^2$  (loi d'anneau produit)
- ③ Résoudre  $x^3 - 3x + 27 \equiv 0 \pmod{1125}$

# Solutions

$$\textcircled{1} \quad n = 2^\alpha \prod_{i=1}^l p_i^{\alpha_i} \quad \text{où } p_i \in \mathcal{P} \text{ et } p_i \neq 2$$

On cherche l'existence de  $k$  tel que  $u(\mathbb{Z}/n\mathbb{Z}) \xrightarrow{\varphi} (\mathbb{Z}/2\mathbb{Z})^k \quad (k \neq 0)$

Si  $\varphi$  existe, Card  $u(\mathbb{Z}/n\mathbb{Z}) = 2^k$

$\Downarrow$

$$\varphi(n) = 2^k$$

$$\text{Or } \varphi(n) = 2^{\alpha-1} \prod_{i=1}^l p_i^{\alpha_i-1} (p_i-1)$$

$$\varphi(n) = 2^k \Rightarrow p_i \mid 2^k \Rightarrow p_i = 2 \text{ ou } 1, \text{ impossible}$$

Si  $\alpha_i > 1$  (Th. Gauss)

Nécessairement, si  $\varphi$  existe,  $\alpha_i = 1$ .

Supposons donc que  $n = 2^\alpha \prod_{i=1}^l p_i$

Nous avons :  $u(\mathbb{Z}/n\mathbb{Z}) \simeq u(\mathbb{Z}/2^\alpha\mathbb{Z} \times \mathbb{Z}/p_1\mathbb{Z} \times \dots \times \mathbb{Z}/p_l\mathbb{Z})$

(th. chinois)

12

$$u(\mathbb{Z}/2^\alpha\mathbb{Z}) \times \prod_{i=1}^l u(\mathbb{Z}/p_i\mathbb{Z})$$

On sait que :

Rappel  $u(\mathbb{Z}/2^\alpha\mathbb{Z}) \simeq \mathbb{Z}/2^{\alpha-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad \text{si } \alpha \geq 3$

$$u(\mathbb{Z}/2^2\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$$

$$u(\mathbb{Z}/2\mathbb{Z}) \simeq \{0\}$$

$$\forall p \in \mathcal{P} \setminus \{2\} \quad u(\mathbb{Z}/p\mathbb{Z}) \simeq \mathbb{Z}/\varphi(p)\mathbb{Z}$$

Donc, si  $\alpha \geq 3$

$$U(\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/2^{\alpha-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \prod_{i=1}^l \mathbb{Z}/\varphi(p_i)\mathbb{Z} \xrightarrow{\varphi} (\mathbb{Z}/2\mathbb{Z})^k$$

Tous les éléments de  $(\mathbb{Z}/2\mathbb{Z})^k$  sont d'ordre 1 ou 2.

$\mathbb{Z}/2^{\alpha-2}\mathbb{Z}$  est cyclique. Il existe  $a \in \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$  d'ordre  $2^{\alpha-2} > 2$ . Donc

$(a, 0, \underbrace{0, \dots, 0}_{l \text{ fois}}) \in \mathbb{Z}/2^{\alpha-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \prod_{i=1}^l \mathbb{Z}/\varphi(p_i)\mathbb{Z}$  est un élément d'ordre  $2^{\alpha-2} > 2$ .

ce qui montre qu'il n'y a pas d'isomorphisme  $\varphi$  (qui conserverait les ordres!)

• si  $\alpha > 3$ ,  $\exists \varphi$

$\alpha = 3, p_i = 3 \Rightarrow n = 2^3 \times 3$  et sa marche,  $n = 2^3$  m. dem. que ci-dessus

Si  $\alpha = 2$

$$U(\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \times \prod_{i=1}^l \mathbb{Z}/(p_i-1)\mathbb{Z} \xrightarrow{\varphi} (\mathbb{Z}/2\mathbb{Z})^k$$

On fait encore un argument d'ordres:

$\forall a \in (\mathbb{Z}/2\mathbb{Z})^k, \omega(a) = 1 \text{ ou } 2$ .

•  $b \in \mathbb{Z}/2\mathbb{Z} \times \prod_{i=1}^l \mathbb{Z}/(p_i-1)\mathbb{Z}$  et  $\omega(b) = p_i - 1$   $\left\{ \begin{array}{l} \varphi \text{ existe} \\ \Downarrow \\ p_i - 1 = \frac{1}{2} \text{ ou } 2 \end{array} \right. \Rightarrow \left\{ \begin{array}{l} p_i = 2, \text{ non} \\ \text{ou} \\ p_i = 3. \end{array} \right.$

Nécessairement,  $p_i = 3$ . (si  $p_i$  existe)

Alors  $U(\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq (\mathbb{Z}/2\mathbb{Z})^2$  convient.

Si  $\alpha = 2$  :  $\left\{ \begin{array}{l} n = 2^2 \times 3 \Rightarrow \exists \varphi (k=2) \\ n = 2^2 \text{ oui} \\ n \neq 2^2 \times 3 \Rightarrow \nexists \varphi \end{array} \right.$

$$\boxed{\text{Si } \alpha = 1}$$

$$U(\mathbb{Z}/n\mathbb{Z}) \simeq \prod_{i=1}^l \mathbb{Z}/(p_i-1)\mathbb{Z}$$

De la m façon que précédemment, on montre que  $\varphi$  existe  $\Rightarrow p_i = 3$ .

Plus, inversement, si  $p_i = 3$   $n = 2 \cdot 3 \Rightarrow U(\mathbb{Z}/_{2,3}\mathbb{Z}) \simeq (\mathbb{Z}/_2\mathbb{Z})^2$  oui.

$$\boxed{\begin{array}{l} \text{Si } \alpha = 1 \\ n = 2 \cdot 3 \Rightarrow \exists \varphi \quad (k=2) \\ n \neq 2 \cdot 3 \Rightarrow \nexists \varphi \end{array}}$$

$$\boxed{\text{Si } \alpha = 0}$$

$p_i = 3$  et alors  $U(\mathbb{Z}/_3\mathbb{Z}) \simeq \mathbb{Z}/_2\mathbb{Z}$ .

sa marche.

$$\underline{\text{Cd}} \quad \exists k \in \mathbb{N}^* / \quad U(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/_2\mathbb{Z})^k$$

$$\text{ssi} \quad \left\{ \begin{array}{ll} n = 2^2 \times 3 & \text{alors } k = 3 \\ n = 2^3 & \text{alors } k = 2 \\ n = 2^2 \times 3 & \text{alors } k = 2 \\ n = 2^4 & \text{alors } k = 1 \\ n = 2 \times 3 & \text{alors } k = 1 \\ n = 3 & \text{alors } k = 1 \end{array} \right.$$

$$(2) \alpha) \quad \mathbb{R}[X] \xrightarrow{\varphi} A$$

A un polynôme de  $\mathbb{R}[X]$ , on peut toujours associer sa valeur en un point d'un  $\mathbb{R}$ -algèbre.

Soit  $(1_A, a)$  une base de  $(A, +, \cdot)$

Définissons  $\varphi$  par : 
$$\begin{cases} \varphi(1) = 1 \\ \varphi(X) = a \end{cases} \quad \text{et} \quad \boxed{\varphi(P) = P(a)}$$

$\varphi$  est un morphisme d'algèbre

$\varphi$  est surjectif car les éléments de la base sont atteints

$\text{Ker } \varphi = \{P / P(a) = 0\}$  est un idéal de  $\mathbb{R}[X]$ . Le seul problème est de montrer q'  $\deg P = 2$ . (où  $(P) = \text{Ker } \varphi$ )

$$\begin{array}{ccc} \mathbb{R}[X] & \xrightarrow{\varphi} & A \\ \pi \downarrow & \nearrow \tilde{\varphi} \text{ isomorphisme d'ev.} & \\ \mathbb{R}[X]/(P) & & \end{array}$$

$$\dim \mathbb{R}[X]/(P) = \dim A \Rightarrow \boxed{\deg P = 2} \quad (\text{cf. Th.})$$

$$\text{Th.} \quad \left| \begin{array}{l} k \text{ corps, } P \in k[X] \\ \text{Alors } \dim_k \mathbb{R}[X]/(P) = \deg P \end{array} \right.$$

(Sol : exhiber une base  $(1, \dots, X^{n-1})$ )

B)

$$\mathbb{C}, \mathbb{R} \times \mathbb{R}, \text{ où } (a, b)(a', b') = (aa', bb')$$

$$\mathbb{R} \oplus \mathbb{R} \epsilon = \mathbb{R} \times \mathbb{R} \quad \text{où} \quad (a, b)(a', b') = (aa', ab' + a'b)$$

$$\begin{cases} (1, 0) = 1 \\ (0, 1) = \epsilon \end{cases} \quad a + b\epsilon \quad \epsilon^2 = 0$$

(cf. les développements limités : pour en faire le produit on se fait d'abord normalement puis on tronque ce qui se passe. Tronquer ça revient à faire  $\epsilon^2 = 0$ )

$\delta = \text{discriminant de } P.$

• Si  $\Delta > 0$   $P = (X - \alpha)(X - \beta)$   $\alpha \neq \beta$   
 $\alpha, \beta \in \mathbb{R}.$

$$\Delta(X - \alpha, X - \beta) = 1 \Rightarrow \mathbb{R}[X] / (P) \underset{\text{anneau}}{\simeq} \mathbb{R}[X] / (X - \alpha) \times \mathbb{R}[X] / (X - \beta)$$

(Th. Chinois)  $\downarrow \quad \downarrow$

$$\Rightarrow \mathbb{R}[X] / (P) \underset{\text{alg}}{\simeq} \boxed{\mathbb{R} \times \mathbb{R}} \not\simeq \mathbb{R}$$

$\mathbb{R} \xrightarrow{Q} \mathbb{Q}(a)$   $\mathbb{R} \xrightarrow{Q} \mathbb{Q}(b)$

• Si  $\Delta = 0$   $P = (X - \alpha)^2$

$$\mathbb{R}[X] / (P) \simeq \boxed{\mathbb{R}[X] / X^2}$$

$$\overline{P(X)} \xrightarrow{\varphi} \overline{P(X + \alpha)}$$

• Si  $\Delta < 0$   $A \simeq \mathbb{R}\mathbb{C}$

(à continuer...)

Fin

③  $x^3 - 3x + 27 \equiv 0 \quad [1125] \quad (1)$

$$1125 = 5^3 \times 3^2$$

$$x^3 \equiv 0 \quad [3] \Rightarrow 3 \mid x^3 \Rightarrow 3 \mid x \quad (3 \in \mathcal{P})$$

Posons  $x = 3\lambda$

Alors (1)  $\Leftrightarrow$  (2) :  $3\lambda^3 - \lambda + 3 \equiv 0 \quad [5^3]$

et on continue (cf. lecteur qui passe, souviens-toi).

## M.1 ALGÈBRE

## 3ème PARTIEL

\* (I) Pour quels couples  $(a, b)$  de nombres complexes la matrice

$$\begin{pmatrix} 0 & a \\ a & 2b \end{pmatrix}$$

est-elle diagonalisable ?

\* (II) Soient  $A$  et  $B$  deux matrices carrées d'ordre  $n$  à coefficients dans le corps commutatif  $K$

1) Montrer que  $AB$  et  $BA$  sont semblables si  $A$  ou  $B$  est inversible.

2) En déduire que les polynômes caractéristiques de  $AB$  et  $BA$  sont égaux - sans hypothèse sur  $A$  ou  $B$ .

3) Donner un exemple ( $n = 2$ ) de couple de matrices  $A$  et  $B$  tel que  $AB$  et  $BA$  ne soient pas semblables.

(III) Soit  $V$  un  $K$ -espace vectoriel de dimension  $n$ , et soit  $u$  un endomorphisme de  $V$ . On dira que  $u$  est monogène s'il existe un vecteur  $e$  de  $V$  tel que

$$e_1 = e, \quad e_2 = u(e_1), \quad \dots, \quad e_k = u(e_{k-1}), \quad \dots, \quad e_n = u(e_{n-1})$$

soit une base de  $V$ .

1) Montrer que le polynôme minimal d'un endomorphisme monogène est de degré  $n$

2) Etudier la réciproque.

3) Donner un exemple d'endomorphisme non monogène

4) Si  $n = 2$ , caractériser les endomorphismes non monogènes.

5) Que peut-on dire des valeurs propres (dans une extension convenable de  $K$ ) d'un endomorphisme monogène diagonalisable ?

Donner des exemples en dimension 3 d'endomorphismes non bijectifs, monogènes et non monogènes.

(IV) Soit  $M$  une matrice carrée d'ordre trois sur un corps  $K$  de caractéristique convenable. Exprimer le polynôme caractéristique de  $M$  en fonction des nombres  $\alpha = \text{tr}(M)$ ,  $\beta = \text{tr}(M^2)$ ,  $\gamma = \text{tr}(M^3)$ ; on précisera le sens de l'adjectif "convenable" utilisé.

DOCUMENTS AUTORISES

Les exercices I , II , III , IV sont indépendants ; il sera tenu le plus grand compte de la clarté des raisonnements.

I Un ordinateur californien, aidé de quelques étudiants, vient d'établir que le nombre

$$2^{21701} - 1$$

2pts

est premier ("le Monde" du 6.12.1978)

Le nombre 21701 est-il premier ?

II

1pts

a) La fonction d'Euler  $\varphi : \mathbb{N}^* \rightarrow \mathbb{N}$  est-elle injective ?

b) Montrer que la fonction

b) Montrer que la fonction

3pts

$$n \rightarrow n \cdot \varphi(n)$$

est injective. On pourra raisonner par récurrence en divisant par le plus grand nombre premier qui divise  $n$ .

III

5pts

Pour quelles valeurs de  $n$  le nombre  $C_n^k$  est-il impair pour tout  $k$  compris entre 1 et  $n$  ?

IV

Soit  $G$  le groupe des matrices  $2 \times 2$  inversibles à coefficients dans le corps  $\mathbb{Z} / 3\mathbb{Z}$ .

1pt

1/ Montrer que  $G$  n'est pas commutatif

2pts

2/ Montrer que l'espace vectoriel  $(\mathbb{Z} / 3\mathbb{Z})^2$  sur le corps  $\mathbb{Z} / 3\mathbb{Z}$  contient 8 vecteurs non nuls et 4 droites vectorielles. Montrer que  $\# G = 48$ .

3/ Définir au moyen de l'action évidente de  $G$  sur les droites vectorielles un homomorphisme  $\rho : G \rightarrow \mathcal{S}_4$

3pts

4/ Montrer que  $\rho$  est surjectif. Quel est son noyau ?

2pts

5/ Montrer que tout élément de  $\mathcal{S}_4$  est d'ordre 1, 2, 3 ou 4.

6/ En déduire que tout élément de  $G$  est d'ordre 1, 2, 3, 4, 6 ou 8. Donner un exemple de matrice de  $G$  correspondant à chaque cas.



Jeudi 22 Mars 1979

Les parties I, II, III sont indépendantes. Le mot "entier" désigne un élément de  $\mathbb{Z}$ .

I a) Déterminer l'ensemble des solutions entières du système :

$$x + y + z = 1$$

$$x + 3y + z = 7$$

b) A quelle condition sur les entiers  $a, b, c$  le système

$$x + y + z = \alpha$$

$$ax + by + cz = \beta$$

admet-il des solutions entières quels que soient les entiers  $\alpha$  et  $\beta$  ?

c) Existe-t-il des triplets d'entiers  $(a, b, c)$  tels que le système<sup>1</sup>

$$\begin{cases} x + y + z = \alpha \\ ax + by + cz = \beta \\ a^2x + b^2y + c^2z = \gamma \end{cases}$$

admette une solution entière quels que soient les entiers  $(\alpha, \beta, \gamma)$  ?

II a) Ecrire la matrice de la multiplication par  $X$  dans la  $\mathbb{R}$ -base de  $\mathbb{R}[X] / (X^2 + 1)^2$  définie par :

$$e_1 = 1 \quad e_2 = X \quad e_3 = 1+X^2 \quad e_4 = X(1+X^2)$$

b) Soit  $u$  un endomorphisme de  $\mathbb{R}^4$  dont l'ensemble des valeurs propres dans  $\mathbb{C}$  est  $\{+i, -i\}$ . Montrer qu'il existe une base de  $\mathbb{R}^4$  dans laquelle la matrice de  $u$  est de la forme

.../...

$$\begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & \alpha & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

avec  $\alpha = 0$  ou  $\alpha = 1$ . Préciser le polynôme minimal de  $u$  dans chaque cas.

III

Soit  $\mathbb{Q}$  le groupe additif des nombres rationnels, et  $\mathbb{Z}$  le sous-groupe des entiers. On considère le groupe  $T = \mathbb{Q}/\mathbb{Z}$ .

- Montrer que l'équation  $n \cdot x = 0$  admet exactement  $n$  solutions dans  $T$ , pour tout entier  $n \in \mathbb{N}^*$ .
- Montrer que tout sous-groupe fini de  $T$  est cyclique.
- $T$  est-il cyclique ?  $T$  est-il de type fini ?
- Soit  $n$  un entier positif non nul donné.  
Montrer que l'application

$$\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \longrightarrow & 0 \\ (x, y) & \longmapsto & \frac{xy}{n} \end{array}$$

définit par passage au quotient une application biadditive symétrique :

$$f : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow T$$

- soit  $C_d$  le sous-groupe cyclique d'ordre  $d$ ,  $d|n$  de  $\mathbb{Z}/n\mathbb{Z}$ .

Déterminer le sous-groupe :

$$(C_d)^\perp = \{x \in \mathbb{Z}/n\mathbb{Z} \mid \forall y \in C_d, f(x, y) = 0\}$$

- 1 Soit  $x$  un nombre complexe algébrique (sur  $\mathbb{Q}$ ). Montrer que ses parties réelles et imaginaires sont algébriques (on rappelle que les nombres algébriques forment un sous-corps de  $\mathbb{C}$ ).
- 2 Montrer que  $2 \cos \frac{\pi}{5}$  et  $2 \sin \frac{\pi}{5}$  sont respectivement racines des polynômes
 
$$P_1(X) = X^4 - 3X^2 + 1$$

$$P_2(X) = X^4 - 5X^2 + 5$$
- 3 Montrer que  $P_1$  n'est pas irréductible sur  $\mathbb{Q}$ , mais que  $P_2$  l'est.
- 4 Déterminer le groupe de Galois de  $P_1$  (sur  $\mathbb{Q}$ ).
- 5 On pose  $r_1 = 2 \sin \frac{\pi}{5}$ ,  $r_2 = 2 \sin \frac{3\pi}{5}$ . Quelles sont les racines de  $P_2$  dans  $\mathbb{R}$  ?
- 6 Montrer que  $\mathbb{Q}(r_1)$  est le corps des racines de  $P_2$ . En déduire l'ordre du groupe  $\text{Gal}_{\mathbb{Q}}(P_2)$ .
- 7 Montrer que  $r_1 \mapsto r_2$  définit un élément d'ordre 4 de  $\text{Gal}_{\mathbb{Q}}(P_2)$ . Conclure.
- 8 Montrer (sans calcul) que  $r_1^2 + r_2^2 \in \mathbb{Z}$ .  
En déduire qu'il existe des polynômes  $P \in \mathbb{Q}[X]$  tels que

$$P^2 \equiv 5 - X^2 \pmod{(X^4 - 5X^2 + 5)}$$

et les trouver tous.

NOTE : Le résultat de la question

1

n'est pas utilisé dans la suite.